



Universidad
Carlos III de Madrid
www.uc3m.es

Diseño e implementación de un sistema de descubrimiento de servicios de red basado en ANQP e IEEE 802.21

Autor: Oliver Caballero Álvarez
Titulación: Grado en Telemática
Director: Antonio de la Oliva Delgado
Tutor: Antonio de la Oliva Delgado
Fecha: 3-6-2013

*Para mis padres, mi hermano
y sobre todo, para ti.*

ABSTRACT

En la sociedad el uso de las redes inalámbricas se ha extendido de forma notoria, permitiendo que cada usuario pueda acceder a todo tipo de servicios de forma continuada.

El desarrollo de tecnologías Wireless Local Area Network (WLAN) como WiFi, Wide Wireless Area Network (WWAN) como GPRS, GSM o UMTS y Wireless Metropolitan Area Network como WiMAX permiten a los usuarios acceder a dichos servicios desde cualquier lugar y momento, paradigma conocido en el mundo anglosajón como “anywhere anytime connectivity”.

Dichas tecnologías utilizan el espectro radioeléctrico para la comunicación y como tal, el servicio sólo se encuentra disponible en un área de cobertura limitada. El movimiento del usuario, al cruzar el límite de cobertura de una celda, hace que sea necesario de realizar traspasos entre diferentes puntos de acceso, conocidos como handovers. Dependiendo del despliegue tecnológico asociado a dicha zona geográfica, los traspasos pueden ser horizontales u homogéneos, donde el traspaso se realiza entre puntos de acceso de la misma tecnología o verticales u heterogéneos, donde el traspaso ocurre entre diferentes tecnologías.

El traspaso entre redes heterogéneas presenta una serie de retos; como el descubrimiento de las diferentes redes, la necesidad de manejar diferentes tipos de interfaz y las diferentes características de las tecnologías. Dado que el mercado demanda soluciones que permitan el traspaso entre redes heterogéneas y dicho traspaso no está exento de problemas, el IEEE aprobó la creación del estándar IEEE 802.21 [1] (Media Independent Handover Services) que define mecanismos para la optimización en el traspaso entre redes heterogéneas. Esta especificación, entre otras cosas, define mecanismos para recibir información sobre las redes existentes en un área geográfica para que el usuario pueda realizar un traspaso. Además, dicha información podría ser muy útil para que el usuario incluso pueda elegir la red que mas le conviene dependiendo de una serie de características elegidas por el mismo.

De esta forma, con los mecanismos propuestos en la especificación IEEE 802.21, un usuario podría informarse de todas las redes a su alrededor. Sin embargo, aunque esta especificación tiene muy buena acogida dentro del mundo académico, no ha sido desplegada mayoritariamente. Uno de los motivos por los que este estándar no ha sido desplegado actualmente es su excesiva complejidad, ya que a parte de los servicios de información referidos anteriormente, también implementa otros servicios como el servicio de comandos y de eventos, siendo todos ellos obligatorios de implementar. Para solventar este problema, el IEEE 802.21 WG está actualmente trabajando en la especificación IEEE 802.21c [2], que permite utilizar un terminal “legacy” para acceder al servicio de información a través de un punto de acceso habilitado a tal efecto.

De esta manera, en este trabajo, exploramos las modificaciones necesarias en los diferentes protocolos utilizados para el intercambio de información entre un terminal de usuario que implemente IEEE 802.11u [3] y un servidor de información IEEE 802.21.

INDICE

1. Introducción	
2. IEEE 802.21: Media Independent Handover Services	
2.1. Descripción general	14
2.2. Media independent event service (MIES)	16
2.3. Media independent command service (MICS)	16
2.4. Media independent information service (MIIS)	17
2.4.1. Elementos de información	19
2.4.2. Protocolo de consulta	20
2.4.3. Representación RDF y consulta SPARQL	21
2.4.3.1. SPARQL	22
2.4.3.2. Ejemplo de consulta al MIIS	23
3. IEEE 802.11u: Interworking with External Networks	
3.1. Introducción	25
3.2. Generic advertisement service (GAS)	25
3.3. Descubrimiento del soporte de 802.11u en APs	26
3.4. Procedimiento del protocolo	27
3.5. Access Network Query Protocol (ANQP)	28
3.5.1. Lista de elementos ANQP	28
4. Trabajo realizado	
4.1. Introducción al problema	30
4.2. Investigación	31
4.3. Desarrollo	31
4.4. Propuestas	31
4.5. Desarrollo	32
4.5.1. Client MIH	33
4.5.2. Client GAS	34
5. Extensión ANQP	
5.1. Introducción	35
5.2. Nuevos elementos ANQP	36
5.2.1. Name network and name network auxiliar	38
5.2.2. Roaming partners	39
5.2.3. Cost network	40
5.2.4. Country code	40
5.2.5. Regulatory domain	41
5.2.6. Capability network	41
5.2.7. QoS	42
5.2.8. IP Configuration	43

5.2.9. Frequency bands	44
5.2.10. PoA	45
6. Pruebas	
6.1. Recopilación de datos entre distintas tecnologías	48
6.2. Descubrimiento de redes wifi	49
7. Conclusiones	
 I. ODTONE	
I.1 Descripción General	52
I.2 Dependencias de ODTONE	52
I.3 Compilación e instalación de ODTONE en GNU/Linux	53
I.4 Estructura de ODTONE	53
 II. SPARQL	
II.1 Generación de base de datos para ODTONE	54
II.2 Consultas SPARQL para cada elemento ANQP	54
 III. Restauración de un linksys WRT546L	
III.1.Linksys WRT546L	59
III.2.Instalación de un nuevo firmware	59

LISTA DE TABLAS

Tabla 1: Elementos de información	19
Tabla 2: consultas SPARQL	20
Tabla 3: Elementos ANQP	28
Tabla 4: Technology	36
Tabla 5: ANQP Ids	37
Tabla 6: Tipo de roaming	39
Tabla 7: Cost Unit	40
Tabla 8: Tipos de CoS	43
Tabla 9: Métodos de configuración	44
Tabla 10: Tipo de link	45
Tabla 11: Tipo de Location	46

LISTA DE FIGURAS

Figura 1: Implementación a desarrollar	13
Figura 2: Movilidad del nodo móvil	15
Figura 3: Protocolo de consulta	20
Figura 4: Consulta RDF	21
Figura 5: Ejemplo RDF	21
Figura 6: Descubrimiento de wifi	26
Figura 7: Intercambio de paquetes GAS	27
Figura 8: Fragmentación de paquetes GAS	27
Figura 9: Red desarrollada	33
Figura 10: Extensión ANQP	35
Figura 11: Elemento ANQP Mejorado	36
Figura 12: Info ID	36
Figura 13: Technology	36
Figura 14: Nuevos elementos	38
Figura 15: Elemento Nombre de la red	38
Figura 16: Elemento Roaming Patners	39
Figura 17: Elemento Patner	39
Figura 18: Elemento Coste de la red	40
Figura 19: Elemento Country code	41
Figura 20: Elemento Regulatory	41
Figura 21: Elemento Regulatory domain	41
Figura 22: Elemento Capacidades de la red	41
Figura 23: Elemento Calidad de servicio	42
Figura 24: Elemento QOS list	42
Figura 25: Elemento CoS	43
Figura 26: Elemento Configuración IP	44
Figura 27: Elemento Bandas de frecuencias	44
Figura 28: Elemento PoA	45
Figura 29: Elemento PoA#N	45
Figura 30: Elemento LinkAddr	45
Figura 31: Elemento Location	46
Figura 32: Elemento Binary Geo Location	46
Figura 33: Elemento Binary Civic Location	46
Figura 34: Elementos XML Location	46
Figura 35: Elemento Channel range	47
Figura 36: Elemento System info	47
Figura 37: Elemento Subnet info	47
Figura 38: Relación entre la extensión ANQP y 802.21 con wifi	48
Figura 39: Relación entre tecnologías 3GPP y las 802 con wifi	49
Figura 40: Relación entre el escaneo de redes wifi y la extensión ANQP	50

LISTA DE ACRÓNIMOS

IEEE	Institute of Electrical and Electronics Engineers
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network
WMAN	Wireless Metropolitan Area Network
GPRS	General Packet Radio Service
GSM	Global System for Mobile
UMTS	Universal Mobile Telecommunications System
WiMAX	Worldwide Interoperability for Microwave Access
ANQP	Access Network Query Protocol
GAS	Generic Advertisement Service
MIHF	Media Independent Handover Function
MIES	Media Independent Event Service
MIIS	Media Independent Information Service
MICS	Media Independent Command Service
RDF	Resource Description Framework
SPARQL	SPARQL Protocol and RDF Query Language
SSPN	Subscription Service Provider Network
IBSS	Independent Base Station Subsystem

LISTA DE REFERENCIAS

- [1] IEEE 802.21: Media independence beyond handover (doi: <http://dx.doi.org/10.1016/j.csi.2011.03.001>) Antonio de la Oliva, Ignacio Soto, Albert Banchs, Johannes Lessmann, Christian Niephaus, Telemaco Melia
- [2] IEEE P802.21c™/D03, Draft Amendment to Standard for Local and Metropolitan Area Networks-Part 21: Media Independent Handover Services. Amendment 3: Optimized Single Radio Handovers.
- [3] IEEE P802.11u™/D3.0, Draft Amendment to Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements; Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 7: Interworking with External Networks.
- [4] IEEE Std 802®-2001, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture.
- [5] IEEE Std. 802.15 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification for Low-Rate Wireless Personal
- [6] IEEE Std 802.11™-2007, Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
- [7] IEEE Std 802.16™-2004 [ISO/IEC 8802-16: 2004], Information Technology—Telecommunications and information exchange between system—Local and metropolitan area networks—Specific equirements—Part 16: Air Interface for Fixed Broadband Wireless Access Systems.
- [8] W3C World Wide Web Consortium. (2007). "SPARQL Query Language for RDF." Retrieved 10/08/2007, from <http://www.w3.org/TR/rdf-sparqlquery/#basicpatterns>.

CAPITULO 1

INTRODUCCIÓN

Los nuevos avances de las tecnologías de software y hardware en telecomunicaciones, están construyendo una nueva generación de herramientas tecnológicas que están generando un inmenso impacto dentro del sector empresarial. Estas nuevas tecnologías permiten a los usuarios con dispositivos móviles conectarse a Internet a una gran velocidad a través de una red de comunicación móvil o a través de redes locales inalámbricas.

Dentro de este nuevo escenario, el término “Tecnología móvil” hace referencia al conjunto de dispositivos y herramientas que nos dan la posibilidad de realizar una actividad determinada de manera que no nos encontremos en el mismo lugar.

Estos avances tecnológicos han impulsado a la sociedad actual a inclinarse con una confianza creciente hacia las distintas posibilidades de explotar servicios hasta hace poco desconocidos, como puede ser el comercio electrónico, el cual está demostrando las innumerables ventajas que este puede aportar al crecimiento económico. Los requerimientos de la población de la sociedad en cuanto al acceso remoto a la información contenida en bases de datos también ha mostrado una evolución creciente, por lo tanto es de interés estudiar y aportar soluciones a medida para brindar servicios que permitan satisfacer estos requerimientos de información.

La utilización del teléfono móvil ha traspasado fronteras inimaginables aportando la libertad de la “no dependencia” de cables para que las personas puedan comunicarse o acceder a Internet en casi cualquier lugar. Las distintas redes existentes proporcionan la cobertura necesaria para que los usuarios tengan siempre un punto de acceso a la red que les permita acceder a los distintos servicios proporcionado por los operadores.

Cuando un usuario ha iniciado una conexión es necesario que ésta se mantenga mientras se desplaza. Puede ocurrir que durante ese desplazamiento el usuario se salga de la zona de cobertura de la red que le da servicio con lo que si antes de que ocurra no se realiza un traspaso de dicha comunicación ésta se acabaría con el consiguiente perjuicio para el usuario. Para que esto no suceda existen los mecanismos de handover que hacen el traspaso de la comunicación de un punto de acceso que va a dejar de estar disponible a otro que puede seguir proporcionando los recursos para que siga la comunicación.

Un handover se define como un proceso en el cual un nodo móvil intercambia el punto de acceso en el que se encuentra conectado con el objetivo de mejorar sus prestaciones. Estos handover pueden realizarse entre puntos de acceso del mismo tipo de enlace o tecnología, los cuales denominaremos como handovers horizontales, o entre puntos de acceso de diferentes tecnologías, los cuales se denominaran handover verticales.

La realización de un traspaso entre tecnologías en un dispositivo supone un tiempo en el cual pierde la conexión. Esto quiere decir que si tuviéramos una videollamada, esta se cortaría al realizar un handover. Para ello, se define el estándar IEEE 802.21.

El estándar IEEE 802.21 define mecanismos que permiten la optimización de traspaso entre redes heterogéneas. Estos mecanismos se basan en el intercambio de paquetes para obtener información y realizar el handover de la forma mas rápida posible lo que reduciría al máximo el tiempo en el que no se esta conectado a una red.

Este estándar, también conocido como Media Independent Handover Services (MIHS), tiene como propósito mejorar la experiencia del usuario para el handover entre redes, especialmente entre aquellas que poseen diferentes tipos de medios y que pertenecen a la familia 802, incluidas redes inalámbricas y cableadas, lo que, a su vez, garantiza coexistencia con tecnologías celulares. Para ello proporciona una funcionalidad MIH (Media Independent Handover) que facilita los procesos de handover iniciados tanto por el móvil como por la red.

IEEE 802.21 garantiza el handover en redes heterogéneas, puesto que soporta y define un marco de trabajo para proveer información intercambiable y actualizada en cuanto a las condiciones del enlace y características de las redes disponibles, al igual que en un conjunto de componentes funcionales para tomar y ejecutar decisiones de movilidad y garantizar el mejor aprovechamiento de las diferentes redes a las que tengan acceso los usuarios en un momento determinado.

Siendo así, el usuario tendría la posibilidad de poder recibir mayor información sobre las redes que se encuentran a su alrededor. Como se ha comentado, el estándar 802.21 define una infraestructura de servicios para la optimización del proceso del handover, los cuales proceden de elementos de la red diferentes al del nodo móvil. De cara al nodo móvil, utiliza solo una parte muy pequeña de la implementación.

De esta forma, es evidente destacar que la implementación de IEEE 802.21 en cada uno de los nodos resulta muy costosa en comparación con el uso que se va a realizar de ella. Por esta razón se busca una posible solución a la capacidad de recibir la información sobre las redes que rodean al nodo móvil sin tener que implementar un estándar tan pesado como el 802.21 para el nodo móvil.

Para ello, el estándar IEEE 802.11u recoge la posibilidad de utilizar un punto de acceso que fuera capaz de comunicarse con un servidor remoto (que podría ser un servidor de información IEEE 802.21) para que mediante el protocolo ANQP, acelerar el descubrimiento de las redes vecinas. Esto supondría no tener que implementar toda la implementación 802.21 en los nodos móviles para poder intercambiar información sobre las redes disponibles.

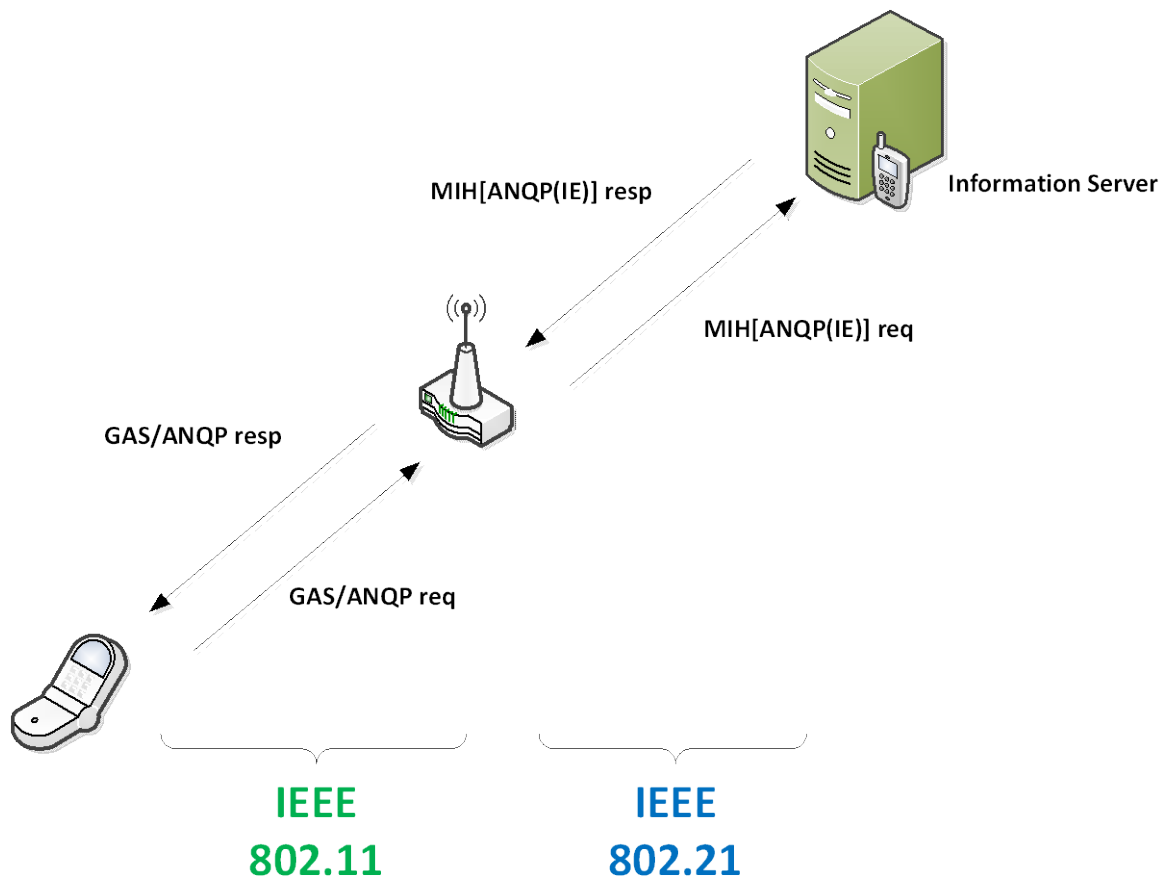


Figura 1: Implementación desarrollada

Sin embargo este estándar supone como perfecto el mapeo de entre los paquetes ANQP y los paquetes 802.21 y además supondría la integración de nueva infraestructura (servidor ANQP).

Como dicho estándar 802.21c esta en proceso todavía en la actualidad, durante este trabajo vamos a realizar un estudio de los estándares 802.21 y 802.11u para buscar una alternativa posible a la recepción de información en el nodo móvil, donde intentaremos realizar un intercambio de paquetes ANQP entre el nodo móvil y el punto de acceso, y el punto de acceso intercambiara paquetes 802.21 como se muestra en la Figura 1.

CAPITULO 2

IEEE 802.21: Media Independent Handover Services

2.1 Descripción general:

El estándar IEEE 802.21 define mecanismos de acceso que permiten la optimización de traspaso entre redes heterogéneas IEEE 802[4] y 3GPP/3GPP2. Su principal propósito es mejorar la experiencia del nodo móvil facilitando la movilidad entre redes de diferentes tecnologías, incluyendo redes cableadas e inalámbricas, donde el intercambio de paquetes no esta definido, y realizando dicha entrega de forma trasparente para el dispositivo móvil que lo admita. Estos mecanismos también se pueden utilizar para el traspaso entre redes IEEE 802 y redes no IEEE 802 como son las definidas en el 3GPP¹ y el 3GPP2²

Para los nodos móviles, los traspasos de una red a otra pueden ocurrir cuando las condiciones de la conexión inalámbrica varían, debido al movimiento de los usuarios, como se muestra en la Figura 2. Para un nodo móvil estacionario, el traspaso puede deberse a cambios en el entorno, haciendo que otra red sea más atractiva que la actual. En este caso el usuario puede elegir una aplicación que requiere una adaptación de la red actual para proporcionar una tasa más alta, por lo que requeriría un traspaso a otra red, dando en todos los casos en la medida de lo posible una continuidad del servicio.

En general, para el uso de esta especificación, el nodo móvil debe ser multimodal, es decir capaz de soportar múltiples tipos de tecnologías para utilizar la mayor disponibilidad de servicio ya que la red global puede incluir una mezcla de redes de diferentes tamaños, tales como las de IEEE 802.15 [5], IEEE 802.11 [6], IEEE 802.16 [7], 3GPP y 3GPP2 , con superposición de cobertura.

¹ <http://www.3gpp.org/>

² <http://www.3gpp2.org/>

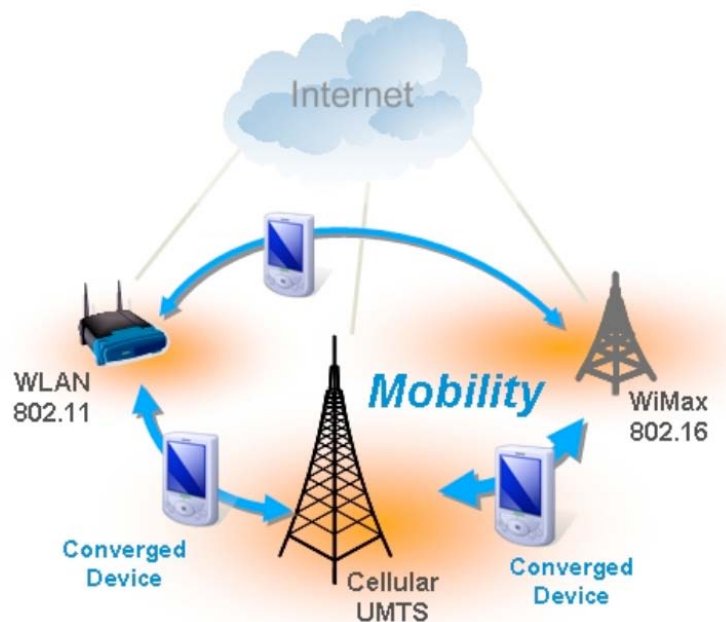


Figura 2: Movilidad del nodo móvil

La especificación esta basada en un Media Independent Handover Function (MIHF) que será una entidad lógica que se encargará de coordinar la información obtenida por las capas inferiores (nivel 1 y 2 de la capa OSI) y facilitará la toma de decisiones. El traspaso en sí y la decisión de realizarlo es tomado por los usuarios MIH, que en la arquitectura móvil actual son los diferentes administradores de conexión de los terminales o agentes de administración en entidades de red. El MIHF proporcionará servicios a las capas superiores de la red, siendo el protocolo específico de cada tecnología de red el que se encargará de comunicarse con las diferentes capas inferiores y gestionar la movilidad entre redes. Cada una de estas tecnologías ha definido mecanismos para facilitar la transferencia horizontal de la información recibida por el MIHF.

Los servicios que componen el MIHF son:

- Media Independent Event Service (MIES), que proporciona la clasificación, filtrado e informe de eventos correspondientes a los cambios dinámicos en las características de las redes.
- Media Independent Command Service (MICS), que permite a los usuarios MIH, administrar y controlar las propiedades del enlace que son relevantes en el traspaso y en la comunicación entre los enlaces.
- Media Independent Information Service (MIIS), que proporciona información detallada sobre las características y servicios proporcionados por las redes vecinas que se utilizará para realizar la decisión más efectiva.

El MIHF proporciona servicios síncronos y asíncronos a través de puntos de acceso a servicios (Service Access Points, SAPs) para los usuarios MIH y sus capas de enlace. En el caso de un sistema con varias interfaces de red de tipo arbitrario, los usuarios MIH utilizarán los servicios descritos anteriormente, proporcionados por el MIHF para administrar, determinar y controlar el estado de las interfaces subyacentes.

Estos servicios proporcionados por el MIHF ayudarán a los usuarios MIH a mantener la continuidad de servicio, adaptación del servicio a la diversa calidad de las

tecnologías de red subyacentes, conservación de la vida de batería, descubrimiento de red y selección de enlace. En un sistema que contiene interfaces de red heterogéneas de tipos de IEEE 802 y celular (3GPP, 3GPP2), el MIHF ayudará a los usuarios MIH en el proceso de handover, mediante una serie de interfaces abstractos comunes a todas las tecnologías soportadas por la especificación.

A continuación detallamos cada uno de los servicios anteriormente mencionados.

2.2 Media independent event service (MIES)

Los handovers pueden ser iniciados por el nodo móvil o por la red. Los eventos relevantes al traspaso se pueden originar en distintos sitios de la red. Por lo tanto, la fuente de estos eventos puede ser local o remota. Se necesita un protocolo de transporte para dar soporte a estos eventos.

Varias entidades de los niveles superiores pueden estar interesadas en estos eventos a la vez. Así, estos eventos pueden tener varios destinatarios. Las entidades de las capas superiores se suscriben para recibir notificaciones de eventos de una fuente en particular. La MIHF ayudará en el envío de estos eventos a los distintos destinatarios.

Los eventos son tratados como eventos discretos. La notificación de los mismos se genera de forma asíncrona. De esta manera, todos los usuarios MIH que quieran recibir notificaciones de eventos necesitan suscribirse a cada evento en particular.

El Event Service se divide en dos categorías, eventos de enlace (Link Events) y eventos MIH (MIH Events). Ambos van desde los niveles inferiores a los superiores. Los eventos de enlace se definen como eventos que se originan en la capa de enlace y física del interfaz de red terminando en el MIHF. Los eventos MIH se definen como eventos que se originan en la MIHF, o son eventos de enlace propagados por la MIHF a los usuarios MIH.

Un evento puede ser local o remoto. Un evento local es el que se propaga entre diferentes niveles dentro de la pila de protocolos local de una entidad MIH, mientras que un evento remoto es el que atraviesa la red de una entidad MIH a otra entidad MIH.

Los eventos de enlace que puede transmitir un MIES son; Link_Detected, Link_Up, Link_Down, Link_Parameters_Report, Link Going_Down, Link_Handover Imminent, Link_Handover_Complete, Link_PDU_transmit_Status. Los eventos MIH que enviara serán: MIH_Link_Detected, MIH_Link_Up, MIH_Link_Down, MIH_Link_Parameters_Report, MIH_Link_Handover Imminent, MIH_Link_Handover_Complete y MIHF_Link_PDU_Transmit_Status.

2.3 Media independent command service (MICS)

El Media Independent Command Service (MICS) hace referencia a los comandos enviados por los usuarios MIH a los niveles inferiores. Los usuarios MIH utilizan el servicio de comandos para determinar el estado de enlaces y/o controlar el dispositivo para un rendimiento óptimo. También permite a los usuarios MIH optimizar las políticas de handover.

Los comandos se clasifican en dos categorías: comandos MIH (MIH Commands) y comandos de enlace (Link Commands).

Los comandos de enlace son originados por la MIHF y dirigidos a los niveles inferiores. Estos comandos controlan principalmente el comportamiento de las entidades de los niveles inferiores. Estos comandos son solamente locales.

Los comandos MIH son generados por los usuarios MIH y enviados a la MIHF. Pueden ser locales o remotos. Los comandos MIH locales son enviados por los usuarios MIH a la MIHF de la pila de protocolos local. Los comandos MIH remotos son enviados por los usuarios MIH a la MIHF de la pila de protocolos asociada. Un comando MIH remoto entregado a la MIHF asociada es ejecutado por los niveles inferiores de la MIHF asociada como un comando de enlace.

Los eventos de enlace que puede transmitir un MICS son `_Link_Capability_Discover`, `_Link_Event_subscribe`, `_Link_Event_Unsubscribe`, `_Link_Get_Parameters`, `_Link_Configure_Thresholds`, `_Link_Action`. Los eventos MIH serán: `MIH_Link_Get_Parameters`, `MIH_Link_Configure_Thresholds`, `MIH_Link_Actions`, `MIH_Net_HO_Candidate_Query`, `MIH_MN_HO_Candidate_Query`, `MIH_N2N_HO_Query_Resource`, `MIH_MN_HO_Commit`, `MIH_Net_HO_Commit`, `MIH_N2N_HO_Commit`, `MIH_MN_HO_Complete` y `MIH_N2N_HO_Complet`.

2.4 Media independent information service (MIIS)

El Media independent information service (MIIS) proporciona un marco que descubre un MIHF, donde residirá el nodo móvil o la red con la que establece conexión y obtiene información de cualquier red de un área geográfica para facilitar la selección y el traspaso a dicha red.

El objetivo de este servicio es adquirir una visión global de todas las redes pertinentes a una zona para facilitar el roaming transparente a través de estas redes para un nodo móvil.

El MIIS incluye soporte para varios elementos de información. Dichos elementos de información proporcionan información esencial para la decisión de selección de red y en el caso de la movilidad del nodo móvil, dichos elementos se utilizarán para dar soporte al roaming a otra red. Dicha información estará disponible en un servidor desde donde el usuario MIH del nodo móvil podrá obtenerla. Los diferentes elementos de información se explicarán en la sección 2.2.2.

El MIIS proporciona la capacidad de obtener información acerca de las capas inferiores de las redes, parámetros de la capa de enlace e información sobre los servicios disponibles de capas superiores como la conectividad a Internet.

El MIIS proporciona un mecanismo genérico para permitir que un proveedor de servicios y un usuario móvil intercambien información sobre diferentes redes de acceso. La información de las redes incluye diferentes tecnologías como redes de 3GPP y 3GPP2 así como de redes IEEE 802.

Los MIIS también permiten acceder a esta información colectiva desde cualquier red, lo que implica que mediante el uso de una red 802.11, el nodo móvil podrá obtener información de no sólo las redes WiFi si no de todas las redes IEEE 802 y las redes 3GPP y 3GPP2; y un nodo móvil conectado a una red 3GPP podrá obtener la

información de cualquier red IEEE 802 en su área geográfica, administrada por su proveedor de acceso. Esta capacidad permite al nodo móvil utilizar su red de acceso para preguntar sobre otras redes de acceso disponibles en una determinada región geográfica. Así, el nodo móvil libera la carga de encendido de cada uno de sus interfaces con el fin de recuperar la información de las redes heterogéneas.

Este servicio de información proporciona principalmente información estática, aunque también se registran cambios de configuración de red. Otra información dinámica acerca de las redes de acceso diferentes, tales como los niveles actuales de recursos disponibles, los parámetros de Estado y estadísticas dinámicas debe obtenerse directamente de las redes de acceso respectivos. Algunas de las principales motivaciones detrás del servicio de información son las siguientes:

- Proporcionar información acerca de la disponibilidad de redes de acceso en una zona geográfica. Además, esta información se puede recuperar utilizando cualquier red inalámbrica o por medio de información que se transmite de manera explícita o implícitamente sobre las redes celulares. Por otra parte, esta información podría mantenerse en una base de datos interna en el nodo móvil.
- Proporcionar información de los parámetros de la capa de enlace que ayudara a los nodos móviles en la selección de la red de acceso adecuado y dará el conocimiento de si la seguridad y calidad de servicio es compatibles con la red de acceso específico.
- Proporcionar información acerca de las capacidades de los puntos de acceso de las diferentes redes para ayudar a la configuración de los interfaces para conectar con las redes de acceso disponibles o seleccionadas. Por ejemplo, da información acerca de los canales configurados en los diferentes puntos de acceso.
- Proporcionar información de los servicios de capas superiores de cada una de las redes. Dicha información no está disponible directamente en la subcapa MAC o PHY de redes de acceso específico, pero puede ser proporcionado como parte del servicio para realizar, por ejemplo, una clasificación de redes diferentes en categorías, como empresa pública, hogar y otros, influyendo así en la decisión de la red a la que contarse.

Es importante señalar que ciertos nodos móviles deben ser capaces de obtener elementos de información relacionada con IEEE 802.21 antes de que el nodo móvil tenga una autenticación con la red. Estos elementos de información se utilizan para la función que determina si se puede seleccionar una red. Para permitir la consulta de información antes de la autenticación, las tecnologías de enlace individuales proporcionan una capa específica para el intercambio de mensajes entre el nodo móvil y las entidades MIHF de la red. Cabe señalar que la facilidad de consulta previa a la autenticación sólo se puede usar para consultas de información y no puede ser utilizada para otros servicios del MIHF.

Permitir el acceso del servicio de información antes de autenticación conlleva ciertos riesgos de seguridad tales como ataques de denegación de servicio o exposición de información a nodos móviles no autorizados. En estos casos el proveedor de servicios de información limita el alcance de la información accesible a un nodo móvil sin autenticar. Después de la autenticación y el apego a un determinado plan de acción, se utiliza el protocolo MIH para la recuperación de información mediante el uso de tramas de datos específicos para cada tecnología.

Al enviar una solicitud o query, el cliente MIIS proporciona un tamaño máximo de respuesta para así limitar el tamaño del mensaje de respuesta. Una solicitud puede contener varias consultas. Si la solicitud contiene varias consultas, estarán en el orden de importancia para el cliente. En el caso de los resultados de la consulta exceden el tamaño máximo de respuesta, se eliminarán los resultados menos significativos de la respuesta. El servidor MIIS tiene su propio límite de tamaño de respuesta máximo configurado que es menor que el especificado por la solicitud del cliente MIIS. En este caso, el mensaje de respuesta devuelve los resultados en el orden de importancia para el cliente hasta ese límite.

2.4.1 Elementos de información

En la Tabla 1, se presentan los diferentes elementos de información disponibles en la especificación, clasificados en tres grupos:

- Información General e información específica de la red de acceso, donde los elementos de información dan una visión general de diferentes redes que proporcionan cobertura dentro de una determinada área geográfica. Por ejemplo, una lista de redes disponibles y sus operadores asociados, acuerdos de roaming entre distintos operadores, el coste de conexión a la red, opciones de seguridad de la red y calidad de servicio. Algunos ejemplos son: IE_NETWORK_TYPE, IE_OPERATOR_ID o IE_NET_CAPABILITIES.
- Información específica del punto de acceso, donde los elementos de información proporcionan información acerca de los puntos de acceso diferentes para cada una de las redes de acceso disponibles. Estos elementos de información incluyen ubicación, velocidad de datos admitidos, tipo de capas física y de enlace y parámetros del canal para optimizar la conectividad. Algunos ejemplos son: IE_POA_LINK_ADDR, IE_POA_LOCATION o IE_POA_ADDR.
- Otra información que es específica de la red de acceso, servicio, proveedor de red. Esta información siempre ira en el elemento de información Vendor Specific.

Información General	
IE_NETWORK_TYPE	Tipo de tecnología utilizada en la red
IE_OPERATOR_ID	Indicador del proveedor de servicio
IE_COUNTRY_CODE	Indicador de código de ciudad
IE_SERVICE_PROVIDER_ID	Indicador del proveedor de servicio
Información específica de la red	
IE_NETWORK_ID	Identificador de acceso a la red.
IE_NETWORK_AUX_ID	Identificador auxiliar de acceso a la red. En el caso de redes 802.11, se referirá al SSID
IE_ROAMING_PARTNERS	Lista de operadores de red con los cuales se puede realizar directamente roaming.
IE_COST	Indica el coste del uso de la red.
IE_NETWORK_QOS	Características de calidad de servicio de la red
IE_NETWORK_DATA_RATE	Máximo valor de tasa de datos que soporta la red
IE_NET_REGULAT_DOMAIN	Dominios regulatorios soportados por la red
IE_NET_FREQUENCY_BANDS	Banda de frecuencias soportadas por la red
IE_NET_IP_CFG_METHODS	Métodos de configuración IP soportados por la red
IE_NET_CAPABILITIES	Capacidades soportadas por la red
IE_NET_SUPPORTED_LCP	Lista de protocolos de localización soportados por la red
IE_NET_MOB_MGMT_PROT	Tipo de protocolo de movilidad soportado por la red

IE_NET_EMSENV_PROXY	Dirección del PSAP (proxy providing access to public safety answering point)
IE_NET_IMS_PROXY_CSCF	IMS proxy P-CSCF
IE_NET_MOBILE_NETWORK	Indicador de movilidad de la red.
Información específica del punto de acceso	
IE_POA_LINK_ADDR	Tipo de tecnología utilizada por el punto de acceso
IE_POA_LOCATION	Localización geográfica del punto de acceso
IE_POA_CHANNEL_RANGE	Rango de frecuencias soportadas por el punto de acceso
IE_POA_SYSTEM_INFO	Información del sistema del punto de acceso
IE_POA_SUBNET_INFO	Información sobre las subredes soportadas por el punto de acceso
IE_POA_IP_ADDR	Dirección Ip del punto de acceso
Otra información	
Vendor specific IEs	Servicios específicos soportados por la red

Tabla 1: Elementos de información

Los elementos de información que transmite el MIIS utilizan dos métodos de representación:

- Una representación binaria, la que conlleva un método de consulta denominado TLV.
- Una representación RDF (Resource Description Framework), que utiliza un método de consulta basado en SPARQL.

2.4.2 Protocolo de consulta

Como se muestra en la figura 3, cuando un usuario MIH requiere información, enviará la primitiva `MIH_Get_Information.request` al MIHF local. Si este dispone de la información solicitada contestará a dicha primitiva con un `MIHF_Get_Information.confirm`. En el caso de que el MIHF no disponga de dicha información, mandará la primitiva al MIIS o a un MIHF Remoto para que el MIIS proporcione dicha información a través de un `MIH_Get_Information.response`.

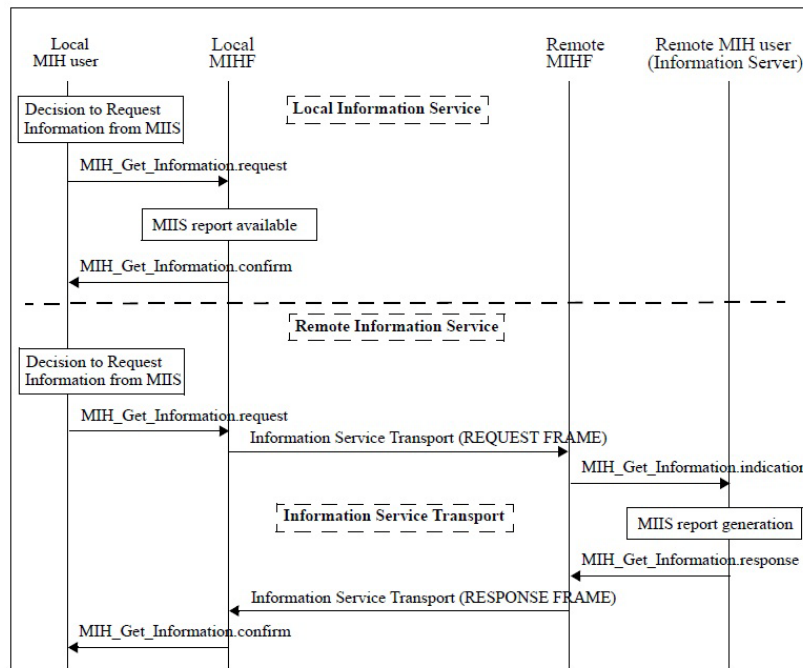


Figura 3: Protocolo de consulta

Las consultas y respuestas incluidas en las primitivas y mensajes MIH_Get_Information, pueden ser codificadas de dos maneras distintas, usando una representación binaria o una representación basada en XML. A lo largo de este trabajo, se ha utilizado la codificación basada en XML, que pasamos a detallar a continuación.

2.4.3 Representación RDF y consulta SPARQL

La representación RDF de los elementos de información se construye en formato XML. Para esto utilizaremos SPARQL como método de consulta. Se usa un esquema en el MIIS de IEEE 802.21 para definir la estructura de cada elemento de información, usándolo también para representar la relación entre ellos.

SPARQL[8] es un lenguaje de consulta para RDF, y actualmente está siendo considerada como una recomendación del W3C para crear un lenguaje de consulta dentro de la Web semántica que está ya implementada en varios lenguajes y bases de datos. Desde 2005 está en proceso de estandarización por el RDF Data Access Working Group (DAWG) del W3C.

RDF (Resource Description Framework) fue el primer estándar definido para la web semántica, posibilitando la descripción de recursos web de manera que sean descifrables por las maquinas. RDF es un lenguaje que define un modelo de datos para describir recursos mediante tripletas sujeto-predicado-objeto o también sujeto-propiedad-objeto.

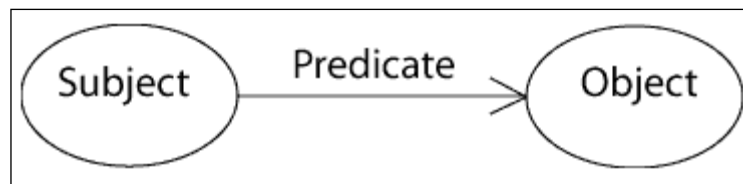


Figura 4: Consulta RDF

El sujeto es el recurso, es decir, es lo que se está describiendo. El predicado es la propiedad o relación que se desea establecer acerca del recurso. Por último, el objeto es el valor de la propiedad o el otro recurso con el que se establece la relación.

La combinación de RDF con otras herramientas como RDF Schema y OWL permite añadir significado a las páginas, y es una de las tecnologías esenciales de la Web semántica.

Hay que tener en cuenta que las URIs juegan un papel importante ya que estas permiten enlazar los recursos con otros a través de sus propiedades.

A continuación se muestra un ejemplo de RDF en modo grafico:

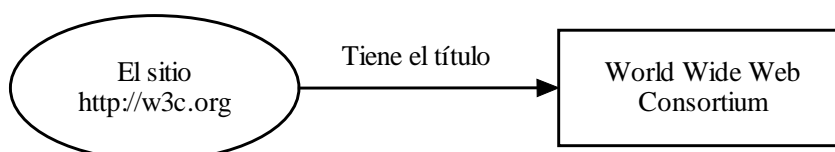


Figura 5: Ejemplo RDF

El mismo ejemplo en versión serializada, sería:

```
...  
<rdf:Description rdf:about="http://w3.org/">  
  <dc:title>World Wide Web Consortium</dc:title>  
</rdf:Description>  
...
```

Considerando que cada recurso tiene asociado un conjunto de metadatos (marcada con etiquetas RDF/XML), entonces tendríamos una gran base de datos formado por ficheros RDF. Viendo esta situación, se hace necesaria una herramienta que permita realizar consultas a dicha base de datos, y optimizar así las búsquedas de información, pero basada en metadatos. Ante esta necesidad el W3C ha propuesto como iniciativa a SPARQL, como un lenguaje de consulta RDF.

Actualmente RDF esta siendo usado para representar información personal, redes sociales, metadatos de recursos web como video, sonido e imágenes, así como para proporcionar un medio de integración entre fuentes de información heterogéneas, siendo su objetivo principal, facilitar la identificación entre recursos web. Entonces con un lenguaje de consulta RDF, como SPARQL, los desarrolladores y usuarios finales se encontrarán con una gran cantidad de información (recursos identificables) teniendo la facilidad para representar y utilizar los resultados obtenidos de manera más eficiente, sustentándose así su utilidad en la necesidad de recuperar y organizar la información de diferentes fuentes.

2.4.3.1 SPARQL

SPARQL tiene especificaciones que explican diferentes partes de su funcionalidad; en general, consiste en un lenguaje de consulta, un formato para las respuestas, y un medio para el transporte de consultas y respuestas:

- SPARQL Query Language: Componente principal de SPARQL. Explica la sintaxis para la composición de sentencias y su concordancia.
- SPARQL Protocol for RDF: Formato utilizado para la devolución de los resultados de las búsquedas (Query SELECT o ASK), a partir de un esquema XML.
- SPARQL Query Results XML Format: Describe el acceso remoto de datos y la transmisión de consultas de los clientes a los procesadores. Utiliza WSDL para definir protocolos remotos para la consulta de bases de datos basadas en RDF.

El lenguaje de consulta SPARQL esta basado en comparación de patrones gráficos. Los patrones gráficos contienen patrones triples. Los patrones triples son como las tripletas RDF, pero con la opción de una variable consulta en lugar de un termino RDF en las posiciones del sujeto, predicado u objeto. Combinando los patrones triples obtenemos un patrón grafico básico, donde es necesario una comparación exacta entre gráficos.

La sintaxis básica de una consulta SPARQL se muestra en la siguiente tabla:

Prologue (optional)	BASE <iri> PREFIX prefix: <iri> (repeatable)
Query Result forms (required, pick 1)	SELECT (DISTINCT)sequence of ?variable SELECT (DISTINCT)* DESCRIBE sequence of ?variable or <iri> DESCRIBE * CONSTRUCT { graph pattern } ASK
Query Dataset Sources (optional)	Add triples to the background graph (repeatable): FROM <iri> Add a named graph (repeatable): FROM NAMED <iri>
Graph Pattern (optional, required for ASK)	WHERE { graph pattern z }
Query Results Ordering (optional)	ORDER BY ...
Query Results Selection (optional)	LIMIT n, OFFSET m

Tabla 2: consultas SPARQL

La función de la palabra clave PREFIX es equivalente a la declaración de espacios de nombres en XML, es decir asocia una URI a una etiqueta, que se usará mas adelante para describir el espacio de nombres. Pueden incluirse varias de estas etiquetas en una misma consulta.

Todo comienzo de una consulta SPARQL queda marcada por la palabra clave SELECT, similar a su uso en SLQ, sirve para definir los datos que deben ser devueltos en la respuesta. La palabra clave FROM identifica los datos sobre los que se ejecutara la consulta, es necesario indicar que una consulta puede incluir varios FROM. La palabra clave WHERE indica el patrón sobre el que se filtraran los tripletes del RDF

2.4.3.2 Ejemplo de consulta al MIIS

Utilizaremos un ejemplo de consulta al MIIS. En este caso utilizaremos una petición para recibir todas las redes disponibles:

```
PREFIX mihbasic: <http://www.mih.org/2006/09/rdf-basic-schema#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
SELECT ?network ?network_aux
WHERE
{
    ?network mihbasic:ie_network_aux ?network_aux .
}
```

Donde una respuesta real seria:

```
<?xml version="1.0" encoding="utf-8"?>
<sparql xmlns="http://www.w3.org/2005/sparql-results#">
  <head>
    <variable name="network_id"/>
```

```
<variable name="network_aux"/>
</head>
<results>
  <result>
    <binding name="network_id"><literal>network1</literal></binding>
    <binding name="network_aux"><literal>aux_id_1</literal></binding>
  </result>
  <result>
    <binding name="network_id"><literal>network2</literal></binding>
    <binding name="network_aux"><literal>aux_id_2</literal></binding>
  </result>
</results>
</sparql>
```


CAPITULO 3

IEEE 802.11u: Interworking with External Networks

3.1 Introducción

Dado que la especificación de la información de servicios proporcionados por la red se encuentra fuera del alcance del estándar 802.11, hay una necesidad de los nodos móviles de preguntar por información sobre servicios de red proporcionados por el subscription service provider network (SSPN) u otras redes externas más allá de un punto de acceso. La característica más importante de este servicio es que el descubrimiento de los servicios de red se realiza antes de asociarse con la red inalámbrica, de manera que el tiempo necesario para seleccionar la red de acceso disminuye considerablemente.

Por esta razón se desarrolla la extensión 802.11u [3] que añade las funciones de:

- Descubrimiento y selección de redes IEEE 802.11.
- Servicios de emergencia
- Distribución de características de calidad de servicio.
- Servicios de interfaz entre el punto de acceso y el SSPN

A lo largo de este trabajo nos vamos a centrar en el descubrimiento y selección de redes IEEE 802.11, que se realiza a través de los protocolos GAS y ANQP, como se detalla en las siguientes secciones.

3.2 Generic advertisement service (GAS)

El protocolo GAS proporciona la funcionalidad que permite a los nodos móviles descubrir la disponibilidad de información relacionada con los servicios de red deseados, Ej., la información sobre servicios que proporciona una IBSS, servicios de acceso locales, proveedores de servicio disponibles de la suscripción (SSPs) y/o SSPNS u otras redes externas. El protocolo GAS usa un contenedor genérico para anunciar la información de los servicios de red sobre una red IEEE 802.11.

En una Independent Base Station Subsystem (IBSS) la funcionalidad del protocolo GAS permite a un nodo móvil tener acceso a la disponibilidad y la información relacionada con servicios deseados proporcionados por otros puntos de acceso en el ESS.

Hay un número de motivos por los cuales el suministro de la información a un nodo móvil en un estado preasociado es beneficioso:

- Esta información apoya la toma de decisión para asociarse a una infraestructura IEEE 802.11. Esto es generalmente más eficiente que el proceso en el que un nodo móvil se asocia a un punto de acceso antes de la obtención de la información y posteriormente decida si hay que quedarse asociado a dicho punto de acceso.
- Para el nodo móvil es posible preguntar por múltiples redes de forma paralela.
- El nodo móvil puede descubrir información sobre los puntos de acceso del mismo grupo administrativo que el punto de acceso al que se encuentra asociado, apoyando la selección de un punto de acceso IEEE 802.11 diferente.

3.3 Descubrimiento del soporte de 802.11u en APs

Para que los puntos de acceso sean detectados, periódicamente, mandan un paquete (cada 100ms, por defecto, aunque es configurable) llamado Beacon Frame donde se encuentra la información suficiente para que los nodos inalámbricos de un área geográfica sepan que existe dicha red, cuál es su identificador y sus características principales. Como se muestra en el intercambio de la Figura 6, los propios nodos móviles pueden enviar un paquete llamado Probe Request Frame donde podrán pedir información sobre dicha red la cual será contestada con un Probe Response Frame.

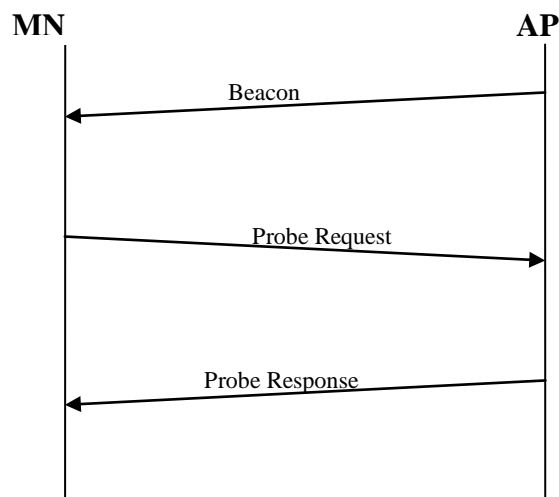


Figura 6: Descubrimiento de wifi

En el caso de GAS, un punto de acceso incluirá un elemento Interworking en cada uno de sus Beacon Frames y de sus Probe Response Frame para indicar que soporta dicho protocolo, mientras que los nodos móviles incluirán el elemento Interworking en su Probe Request Frame. Además, la presencia de un Advertisement Protocol en el Beacon Frame o en el Probe Response Frame indicará que el punto de acceso soporta dicho elemento.

3.4 Procedimiento del protocolo

El protocolo GAS tendrá lugar entre dos estaciones, donde una estación hará una pregunta GAS transmitiendo un frame GAS Initial Request, y la estación receptora transmitirá una respuesta a dicha pregunta con un GAS Initial Response como se muestra en la figura 7. La respuesta a esta pregunta podrá obtenerse de la misma estación receptora (por ejemplo de un caché local), o por medio de algún servidor de información externo, mediante protocolos fuera de la especificación IEEE 802.11.

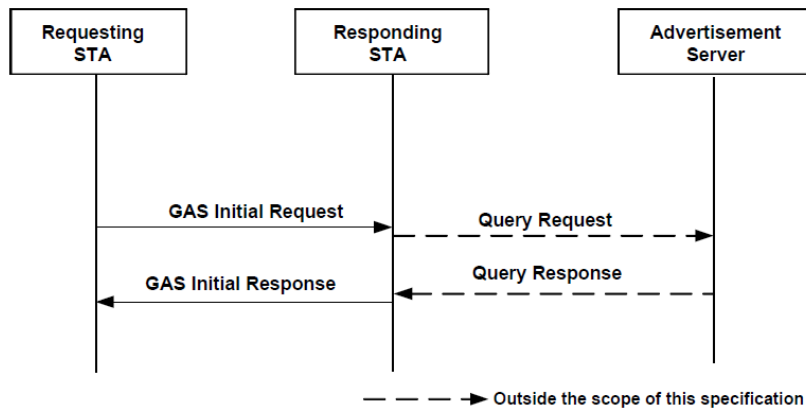


Figura 7: Intercambio de paquetes GAS

Como se muestra en la Figura 8, en el caso de exceder el tamaño de mensaje máximo, el mensaje será fragmentado de tal forma que después del GAS Initial Request, la estación transmisora enviará tantos GAS Comeback Request como sean necesarios, la estación receptora responderá con mensajes GAS Comeback Response.

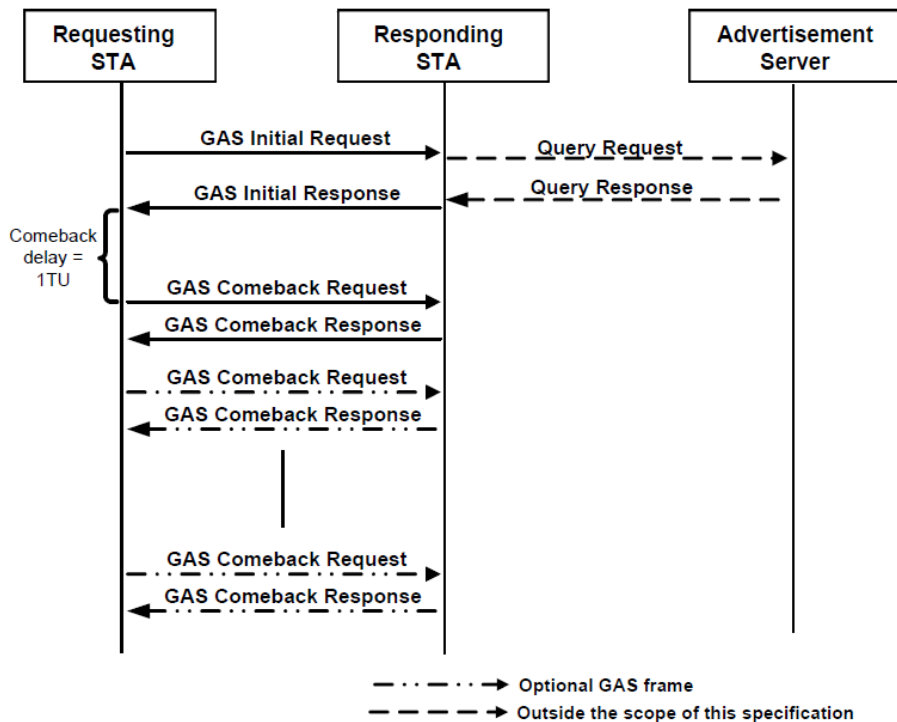


Figura 8: Fragmentación de paquetes GAS

La primera estación preguntara en base al Advertisement Protocol enviado dentro del GAS. Los protocolos que soporta un Advertisement Protocol son los siguientes:

- ANQP, que proporcionara información sobre el punto de acceso con el que estamos estableciendo comunicación.
- MIHF, definido por la especificación 802.21, donde podremos informarnos de las redes dentro de un área geográfica.
- EAS, que mandara mensajes de emergencia a redes externas.

Aunque el protocolo GAS permite la realización de consultas MIHF directamente, el uso de este protocolo impone que el terminal emisor implemente la especificación IEEE 802.21. Tal y como se explicó en la introducción, el soporte de este protocolo en terminales móviles no es algo común. En este trabajo nos centramos en proporcionar información residente en el servidor externo MIIS mediante mensajes del protocolo ANQP. Dicho protocolo será soportado por defecto por todas las estaciones implementando IEEE 802.11u (estaciones que soporten la especificación IEEE 802.11-2012).

3.5 Access Network Query Protocol (ANQP)

Si el “Advertisement Protocol ID” colocado dentro del elemento “Advertisement Protocol” es igual a 0, el paquete GAS proporcionara una pregunta AQNP. Esta pregunta ANQP estará definida en el elemento “Query Request” del paquete GAS. De este modo, el nodo móvil mandara un GAS Initial Request, donde el punto de acceso recibirá la pregunta realizada por el nodo móvil y rellenara un GAS Initial Response con la pregunta realizada en el campo “Query Response”.

Dentro de esa pregunta GAS, el nodo móvil podrá realizar una única, o una lista de preguntas.

3.5.1 Lista de elementos ANQP

Los elementos ANQP se muestran en la Tabla 3:

Nombre	Tipo	Desciption
ANQP Query list	S	Elemento que proporciona una lista de identificadores ANQP los cuales se podrán utilizar para rellenar la query que realizara el STA.
ANQP Capability list	Q	Elemento que proporciona una lista de identificadores ANQP los cuales se utilizaran para que el punto de acceso informe de cuales son elementos ANQP que puede procesar.
Venue Name information	S	Elemento que proporciona 0 o mas “venue names” asociados con el punto de acceso. Un “venue name” informa de una localización cívica la cual proporciona el servicio de la red.
Emergency Call Number information	S	Elemento que proporciona una lista de números de teléfono de emergencias.
Nework Authentication Type information	S	Elemento que proporciona una lista de tipos de autenticación que soporta el punto de acceso.
Roaming Consortium list	S	Elemento que proporciona una lista de roaming que son accesibles a través de redes que son servidas desde este punto de acceso.
IP Address Type Availability information	S	Elemento que informa sobre la versión y el tipo de la dirección IP que podría tener el nodo móvil después de realizar una asociación satisfactoria.
NAI Realm list	S	Elemento que proporciona una lista de identificadores de redes cuyas

		redes o servicios son accesibles vía este punto de acceso.
3GPP Cellular Network information	S	Elemento que proporciona información básica sobre las redes 3GPP.
AP Geospatial Location	S	Elemento que proporciona la localización geoespacial del punto de acceso.
AP Civic Location	S	Elemento que proporciona la localización cívica del punto de acceso.
AP Location Public Identifier URI	S	Elemento que proporciona la localización pública del punto de acceso.
Domain Name list	S	Elemento que proporciona una lista de dominios de redes 802.11 que operan en este punto de acceso.
Emergency Alert Identifier URI	S	Elemento que proporciona una URI que se podrá utilizar para establecer conexión de emergencia
Emergency NAI	S	Elemento que proporciona una string que identifica una red de emergencia.

Tabla 3: Elementos ANQP

Q: El elemento esta en una pregunta ANQP.

S: El elemento esta en una respuesta ANQP.

CAPITULO 4

Trabajo Realizado

4.1 Introducción al problema

Como hemos visto, hoy en día la tecnología inalámbrica nos permite obtener información de todas las redes que tenemos a nuestro alrededor, sin observar la tecnología que estemos utilizando. Incluso sin estar conectados, con la tecnología IEEE 802.11u podríamos obtener información de las redes que da acceso el punto de acceso con el que establecemos comunicación.

Sin embargo, surgen problemas con respecto a la obtención de dicha información:

- En el caso de la implementación de la tecnología 802.21 para obtener información en cada uno de los nodos móviles, supondría la implementación de un estándar muy extenso para solo el uso de una parte muy minúscula, lo que además supondría, que los nodos móviles deberían tener un soporte para dicha tecnología.
- En el caso del uso del protocolo GAS de 802.11, la limitación de su información supone una pérdida en la posibilidad de obtener toda la información posible sobre las redes que tenemos a nuestro alrededor.

De esta forma en este proyecto desarrollaremos una ampliación del protocolo GAS donde introduciremos nuevos elementos ANQP que permitirán descubrir redes externas a través de una red 802.11 sin la necesidad de implementar tecnología 802.21 en el nodo móvil.

Esta ampliación del protocolo GAS-ANQP nos permitirá no solo conocer las redes que da señal el punto de acceso con el que estamos pre-asociados, como nos informaría el protocolo GAS establecido en IEEE 802.11u con el uso de ANQP, si no que nos informaría de todas las redes que se encuentran en una área geográfica, como si fuera IEEE 802.21 pero prescindiendo de dicha tecnología en el nodo móvil.

Esta información nos serviría para presentar una multitud redes a las que el usuario podría llegar a conectarse ya que podríamos conocer todas las redes disponibles, la tecnología que usan, los servicios que ofrecen o la calidad de servicio que proporcionan, por ejemplo, en el caso de un usuario móvil podría ofrecerse todas las redes wifi a las que se puede conectar, pero en vez de ofrecer una lista con todas las SSID de las redes 802.11 podríamos ofrecer una lista de redes que ofrecieran los servicios que el usuario móvil haya configurado en el nodo móvil antes de establecer conexión con ninguna red.

4.2 Investigación

El proceso de investigación de este proyecto ha desarrollado la mayor parte del trabajo realizado.

Esta investigación se ha basado en el estudio de las especificaciones 802.11u y 802.21 para resolver la problemática que surge a la hora de recibir información cuando un nodo móvil intenta informarse sobre las redes que tiene a su alrededor.

4.3 Desarrollo

Una vez echo un estudio sobre los estándares 802.11u y 802.21, se realizan propuestas para recibir la información de MIIS a través del uso de una red IEEE 802.11.

Para establecer conexión con el punto de acceso antes de la autenticación, utilizaremos el protocolo GAS con consultas ANQP, por lo que se decide desarrollar una extensión de dicho protocolo.

4.4 Propuestas

En la primera propuesta, se piensa la posibilidad de rellenar los elementos ANQP ya existentes con información 802.21 en vez de con información proporcionada por el punto de acceso. Una vez se empieza a desarrollar dicha propuesta, se observa que los siguientes inconvenientes:

- La mayoría de los elementos ANQP son destinados a las redes que da servicio el punto de acceso, lo que requeriría un cambio sobre la implementación de la mayoría de los elementos de información, cosa que impediría obtener la información para la cual se habían desarrollado dichos elementos inicialmente.
- Algunos elementos ANQP no pueden ser rellenados con la información que se puede obtener a través de 802.21, lo que requeriría una extensión de la especificación IEEE 802.21, para la creación de nuevos elementos de información que proporcionasen dicha información.

Dicha primera propuesta supone el diseño e implementación de nuevos elementos ANQP, para de esta manera no modificar los elementos de información ya implementados por este protocolo. Esto implica que en la siguiente propuesta se realizará un estudio de toda la información que puede recibir un punto de acceso referente a todas las redes y servicios establecidos dentro del área geográfica en la que se encuentra el nodo móvil.

De esta forma, la propuesta supone la posibilidad de crear nuevos elementos de información ANQP con toda la información recibida del MIIS, generando 10 nuevos elementos ANQP para recibir la información desde el punto de acceso hasta el nodo móvil.

La propuesta establece la posibilidad de recibir en un sólo paquete la información de todas las redes disponibles respecto a una pregunta específica. Sin embargo, la posibilidad de que dentro del área geográfica exista un número muy elevado de redes,

implica que el paquete pueda ser excesivamente grande, lo que supondría un retardo muy elevado en el caso de que queramos hacer una consulta sencilla. Por ejemplo, si quisiéramos saber cuales son las redes 3GPP que se encuentran en nuestra zona geográfica, recibiríamos un paquete con todas las redes disponibles en nuestra zona, sin importar la tecnología que utilizan.

Para solventar este problema, proponemos la introducción de nuevos elementos ANQP, pero en este caso recibiremos información sobre las redes disponibles dentro de un ámbito específico indicado en la pregunta, en este caso solo referente a un tipo de tecnología específica.

Esta nueva propuesta implicara que para recibir información sobre todas las redes existentes, tendríamos que hacer una query por cada una de las tecnologías disponibles, pero de esta forma no recibiríamos información de más, referente a tecnologías que no nos interesan.

Por lo general, un usuario necesita obtener información sobre una lista de redes de la misma tecnología para informarse de cual de ellas ofrece un servicio, calidad de servicio o disponibilidad mejor para su uso, por lo que se establece como solución mas optima esta ultima opción.

4.5 Desarrollo

El desarrollo de este proyecto será la implementación usando el lenguaje de programación C y C++ del protocolo definido anteriormente. Para ello utilizaremos la implementación ya desarrollada ODTONE (ver Anexo I).

Una vez instalado ODTONE, hemos procedido a realizar modificaciones en la implementación C++ del cliente generado por ODTONE y se ha generado una implementación en C que realizara el intercambio de paquetes GAS.

En la Figura 9, se muestra una posible configuración de red que vamos a diseñar, donde el nodo móvil se comportara como lo que denominaremos “cliente GAS”, el punto de acceso 1, al cual el nodo se “pre-conectara”, actuara como “cliente MIH”.

Antes de empezar a describir el trabajo realizado, cabe mencionar que la comunicación establecida entre el nodo móvil y el punto de acceso se ha implementado a nivel 3, dejando la implementación de la comunicación a nivel 2 para un trabajo futuro.

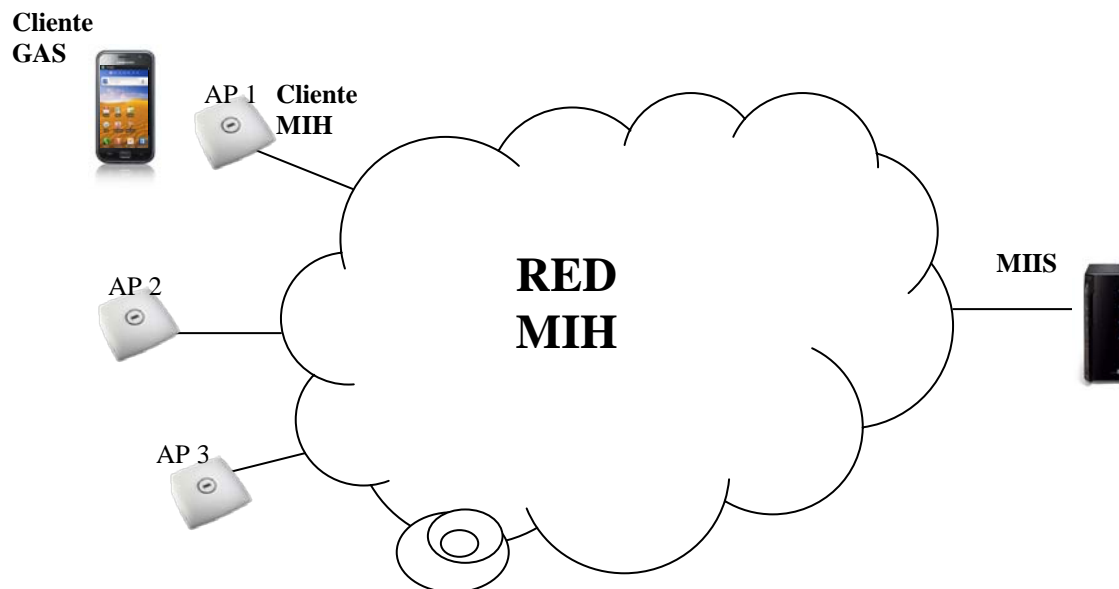


Figura 9: Red desarrollada

4.5.1 Client MIH

En este desarrollo utilizaremos una estructura para el client MIH separada en:

- client.cpp : Archivo fuente que presenta el programa principal
- auxiliar.cpp : Archivo con funciones auxiliares
- anqp.c : Archivo fuente que contiene todos los elementos ANQP
- xml.c: Archivo fuente con funciones auxiliares para la captura de la respuesta SPARQL basada en xml.

Una vez instalado “app/client” de ODTONE, hemos procedido a modificar su función principal alojada en el “client.cpp”. En esta función, generaremos un socket UDP que procesara todos los paquetes que lleguen a nuestra dirección IP en un puerto predeterminado. Una vez que leamos de dicho puerto, verificaremos que el paquete recibido es un paquete GAS. En el caso de que sea un paquete GAS, leeremos el elemento “Advertisement protocol”. Verificando que la pregunta es ANQP la procesaremos y descubriremos cual es la pregunta que ha realizado el nodo móvil. Esta pregunta será transmitida al MIIS a través del MIHF mandando un Get_Iformation_request que se mandara a través de la función ya creada en ODTONE “send_rdf_get_information _request” donde introduciremos la consulta SPARQL correspondiente. (Ver Anexo II.5).

Una vez mandado este mensaje esperará a recibir la respuesta enviada desde el MIIS. Una vez recibamos dicho mensaje, obtendremos un paquete MIH el cual tendrá como datos una estructura XML. Se utilizarán las funciones del archivo fuente “xml.c” para obtener cada una de las respuestas obtenidas de la respuesta para generar la respuesta GAS.

Ya establecida la respuesta crearemos un socket UDP para mandar la respuesta a la dirección la cual había mandado la pregunta.

4.5.2 Client GAS

En este desarrollo utilizaremos una estructura para el client GAS separada en:

- client.c: Archivo fuente que presenta el main principal
- anqp.c: Archivo fuente que contiene todos los elementos ANQP
- gas.c: Archivo fuente con funciones de creación de los paquetes del protocolo GAS.

Generaremos un archivo fuente “client.c” que se ejecutara como un nodo móvil que requiere información. Para ello crearemos un socket UDP que conectaremos con la dirección del cliente MIH donde enviaremos el paquete GAS. Utilizaremos como parámetros el ID de la pregunta ANQP y el ID de la tecnología con los que obtendremos la información. Utilizaremos estos parámetros para crear el elemento ANQP que utilizaremos en el GAS Query.

Una vez mandado este mensaje GAS, crearemos un nuevo socket para la recepción de la respuesta enviada por el cliente MIH. Esta respuesta será procesada y escribirá la respuesta de cada una de las redes en archivos aislados, generando por cada red un archivo llamado “nombre de la red” donde estarán escritas cada uno de los datos obtenidos en la respuesta actual o en respuestas anteriores.

CAPITULO 5

Extensión ANQP

5.1 Introducción

Como ya hemos comentado anteriormente, realizaremos una extensión de protocolo GAS, para ello, introduciremos nuevos elementos ANQP para recibir la máxima información posible sobre todas las redes que están a nuestro alrededor. Para ello realizaremos un intercambio de paquetes antes de la preasociación con el punto de acceso a través del intercambio de paquetes GAS con el punto de acceso, el cual mantendrá un intercambio de paquetes IEEE 802.21 con el servicio MIIS.

Al ser sólo una extensión del protocolo GAS, seguiremos obteniendo del punto de acceso la información referente a su soporte de GAS a través de la presencia en la beacon o en el probe response de un INTERWORKING. En el caso de que aparezca el IE INTERWORKING podremos asegurarnos de que se puede utilizar el protocolo GAS. Además dentro de este IE INTERWORKING sabremos que se puede utilizar ANQP si existe el elemento ADVERTISEMENT.

Siendo así, una vez que el nodo móvil conoce que el punto de acceso tiene la capacidad del protocolo GAS, enviara un GAS Initial Request hasta el punto de acceso con la pregunta ANQP que requiera, dicho punto de acceso obtendrá la información necesaria de si mismo o del MIIS según lo establecido en el estándar 802.21, mandando un MIH_Get_Information request a lo que será contestado con un MIH_Get_Information response. Una vez obtenida dicha información contestara con todos los paquetes GAS necesarios para contestar la pregunta realizada.

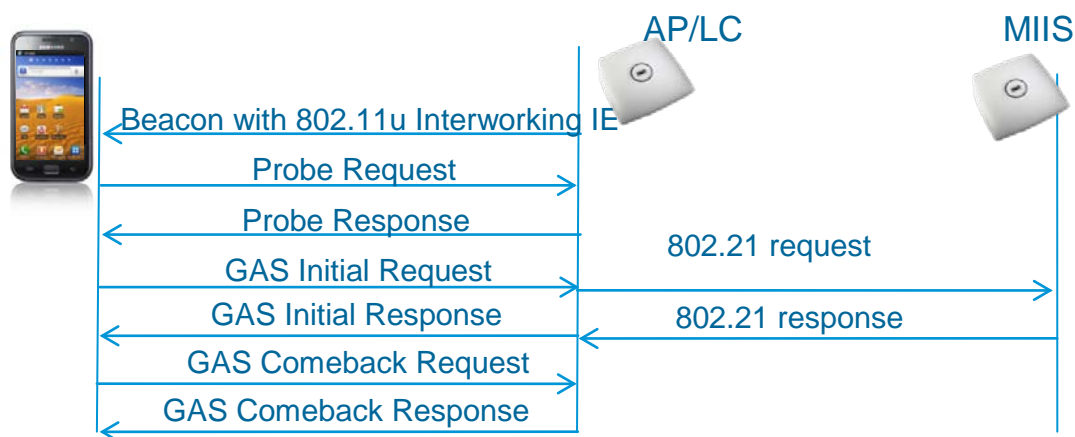


Figura 10: Extensión ANQP

5.2 Nuevos elementos ANQP

El formato del elemento ANQP se presenta en la Figura 11.

	Info ID	Length	Information
Octets:	2	2	variable

Figura 11: Elemento ANQP Mejorado

Donde sustituiremos en todos ellos el campo Info ID por el siguiente, caracterizando así cada uno de los paquetes por su tecnología y su pregunta específica AQNP:

Info ID:

El formato del elemento Info ID se presenta en la Figura 12.

	Tecnology	AQNP ID
Bits:	7	9

Figura 12: Info ID

Donde la tecnología será 0 para los elementos que ya existían, y para donde los nuevos elementos ANQP estará caracterizada por:

Tecnology:

El formato del elemento Info ID se presenta en la Figura 13

	Type	Subtype
Bits:	4	3

Figura 13: Tecnology

Donde cada uno de los parámetros podrá contener los valores de la Tabla 4, donde se especifican cada uno de los tipos y subtipos de tecnología de red:

Type Value	Subtype Value	Type	Subtype
1	0	Wireless - GSM	N/A
2	0	Wireless - GPRS	N/A
3	0	Wireless - EDGE	N/A
4	0	Ethernet - IEEE 802.3	10 Mb
4	1	Ethernet - IEEE 802.3	100 Mb
4	2	Ethernet - IEEE 802.3	1000 Mb
5	0	Wireless – Other	N/A
6	0	Wireless – IEEE 802.11	2.4 Ghz
6	1	Wireless – IEEE 802.11	5 Ghz
6	2	Wireless – IEEE 802.11	4.9 Ghz
6	3	Wireless – IEEE 802.11	3.65 Ghz
6	4	Wireless – IEEE 802.11	3.16 Ghz
7	0	Wireless – CDMA2000	N/A

8	0	Wireless – UMTS	Rel-99
8	1	Wireless – UMTS	Rel-4
8	2	Wireless – UMTS	Rel-5 (w/HSPA)
8	3	Wireless – UMTS	Rel-6 (w/HSUPA)
8	4	Wireless – UMTS	Rel-7 (MIMO/OFDM)
8	5	Wireless – UMTS	Rel-8
9	0	Wireless – cdma2000-HRPD	Rev-0
9	1	Wireless – cdma2000-HRPD	Rev-A
9	2	Wireless – cdma2000-HRPD	Rev-B
9	3	Wireless – cdma2000-HRPD	Rev-C
10	0	Wireless – IEEE 802.16	2.5 Ghz
10	1	Wireless – IEEE 802.16	3.5 Ghz
10	2	Wireless - IEEE 802.20	N/A
10	3	Wireless - IEEE 802.12	N/A

Tabla 4: Tecnology

De esta forma obtendremos con cada pregunta GAS, la información de cada una de las redes cercanas de un tipo de tecnología específico, para no tener una extensión muy grande de paquetes para el caso de preguntas muy específicas.

Además la Tabla 5 indica los nuevos elementos ANQP, modificando su tamaño, ya que ahora el campo “ANQP ID” no utilizara 16 bits si no 9:

Information name	ANQP ID	ANQP information element
Reserved	0-255	N/A
ANQP Query list	256	N/A
ANQP Capability list	257	N/A
Venue Name information	258	N/A
Emergency Call Number information	259	N/A
Network Authentication Type information	260	N/A
Roaming Consortium list	261	N/A
IP Address Type Availability information	262	N/A
NAI Realm list	263	N/A
3GPP Cellular Network information	264	N/A
AP Geospatial Location	265	N/A
AP Civic Location	266	N/A
AP Location Public Identifier URI	267	N/A
Domain Name List	268	N/A
Emergency Alert Identifier URI	269	N/A
TDLS Capability	270	N/A
Emergency NAI	271	N/A
Neighbor Report	272	N/A
ANQP vendor-specific list	477	N/A
Name network and name network auxiliar	273	5.2.1
Roaming patners	274	5.2.2

Cost network	275	5.2.3
Country code	276	5.2.4
Regulatory domain	277	5.2.5
Capability network	278	5.2.6
QoS	279	5.2.7
IP Configuration	280	5.2.8
Frequency bands	281	5.2.9
PoA	282	5.2.10

Tabla 5: ANQP IDs

En la Tabla 5, se han marcado en gris los nuevos elementos introducidos en este trabajo.

Todos los nuevos elementos ANQP tendrán el formato descrito en la Figura 14, donde separaremos cada red de forma aislada para obtener la información de cada una.

	Info ID	Length	Count Net	Length Net #1	Net #1	Length Net #2	Net #2	Length Net #n	Net #n
Oct:	2	2	1	1	variable	1	variable	1	variable

Figura 14: Nuevos elementos

- “Info ID” estará definido por la tabla “ANQP ID”
- “Length” será la longitud del elemento ANQP (1 mas la longitud de cada una de las redes).
- “Count network” será el numero de redes que posee el elemento ANQP.
- “Network #” será la respuesta de cada una de las redes del elemento ANQP requerido.

Para no repetir para cada uno de los elementos de información ANQP, sólo especificaremos el campo “Network” de cada uno de los elementos.

5.2.1 Name network and name network auxiliar:

Este elemento de información nos proporcionara todas los nombres primarios y auxiliares (SSID en el caso de redes 802.11u) de todas las redes de una misma tecnología, especificada en el “Info ID” del elemento ANQP.

Para este elemento utilizaremos el elemento de información especificado en 802.21 proporcionado por el MIIS “IE_NETWORK_ID” y “IE_NETWORK_ID_AUX”. El formato del elemento Nombre y nombres auxiliares de la red se presenta en la Figura 15.

Network #1			
Length name	Name network	Length name aux	Name network aux
Octets: 1	Variable	1	variable

Figura 15: Elemento Nombre de la red

- “Length name” será la longitud del nombre de la red.

- “Name network” será el nombre de la red (definido por la respuesta MIHF “IE_NETWORK_ID”).
- “Length name aux” será la longitud del nombre auxiliar de la red.
- “Name network aux” será el nombre auxiliar de la red (definido por la respuesta MIHF “IE_NETWORK_ID_AUX”).

5.2.2 Roaming patners:

Este elemento de información nos proporcionara una lista de todas las redes con las que el operador del punto de acceso tiene acuerdos de roaming.

Para este elemento utilizaremos el elemento de información especificado en 802.21 proporcionado por el MIIS “IE_ROAMING_PATNERS”. El formato del elemento Roaming patners se presenta en la Figura 16.

Network #1					
Length name	Name network	Count patners	Patner #1	Patner #2 (optional)	Patner #n (optional)
Octets: 1	variable	1	variable	variable	variable

Figura 16: Elemento Roaming Patners

- “Length name” será la longitud del nombre de la red.
- “Name network” será el nombre de la red (definido por la respuesta MIHF “IE_NETWORK_ID”).
- “Count patners” será el numero de redes que podemos hacer roaming desde esta red.
- “Patner #” será la respuesta de cada una de las redes roaming de esta red. El formato se presenta en la Figura 17.
-

Patner #1		
Type	Length	Name
Octets: 1	1	variable

Figura 17: Elemento Patner

- ❖ “Type” será la respuesta MIHF “IE_ROAMING_PATNERS->op_namespace” y su valor estará definido en la Tabla 6.

Tipo	Valor
GSM/UMTS	0
CDMA	1
REALM	2
ITU-T/TBS	3
General	4

Tabla 6: Tipo de roaming

- ❖ “Length” será la longitud del nombre de la red roaming.
- ❖ “Name” será el nombre de la red roaming y estará definido por la respuesta MIHF “roaming_patners->op_name”.

5.2.3 Cost network:

Este elemento de información nos proporcionará el coste de cada una de las redes de la tecnología especificada en el “Info ID” del elemento ANQP.

Para este elemento utilizaremos el elemento de información especificado en 802.21 proporcionado por el MIIS “IE_COST”. El formato del elemento Coste de la red se presenta en la Figura 18.

Network #1					
	Length name	Name network	Cost Unit	Cost Value	Cost Curr
Octets:	1	variable	1	2	1

Figura 18: Elemento Coste de la red

- “Length name” será la longitud del nombre de la red.
- “Name network” será el nombre de la red (definido por la respuesta MIHF “IE_NETWORK_ID”).
- “Cost unit” serán las unidades en las que se medirá “Cost Value” (definido por la respuesta MIHF “IE_COST->cost_unit”).

Unidad	Cost Unit
Second	0
Minute	1
Hours	2
Day	3
Week	4
Month	5
Year	6
Free	7
Flat rate	8

Tabla 7: Cost Unit

- “Cost value” serán el valor del coste de la red en las unidades que indique “Cost unit” (definido por la respuesta MIHF “IE_COST->cost_value”).
- “Cost curr” serán tres letras de correnncy code definidas en ISO 4217 (definido por la respuesta MIHF “IE_COST->cost_curr”).

5.2.4 Country code:

Este elemento de información nos proporcionará el código de la ciudad de cada una de las redes de la tecnología especificada en el “Info ID” del elemento ANQP.

Para este elemento utilizaremos el elemento de información especificado en 802.21 proporcionado por el MIIS “IE_COUNTRY_CODE”. El formato del elemento Country code se presenta en la Figura 19.

Network #1		
Length name	Name network	Country code
1	variable	2

Octets:

Figura 19: Elemento Country code

- “Length name” será la longitud del nombre de la red.
- “Name network” será el nombre de la red (definido por la respuesta MIHF “IE_NETWORK_ID”).
- “Country code” será representado por 2 letras en ISO 3166-1 en capital ASCII letras (definido por la respuesta “IE_COUNTRY_CODE”).

5.2.5 Regulatory domain:

Este elemento de información provee de los “regulatory domain” de cada uno de las redes de una tecnología especificada en el “Info ID” del elemento ANQP. Un “regulatory domain” estará definido por un “country code” y por un “regulatory class” definido en el anexo J de 802.11k.

Para este elemento utilizaremos el elemento de información especificado en 802.21 proporcionado por el MIIS “IE_NET_REGULAT_DOMAIN”. El formato del elemento Regulatory Domain se presenta en la Figura 20.

Network #1		
Length name	Name network	Regulatory domain
1	variable	3

Octets:

Figura 20: Elemento Regulatory

- “Length name” será la longitud del nombre de la red.
- “Name network” será el nombre de la red (definido por la respuesta MIHF “IE_NETWORK_ID”).
- “Regulatory domain” será representado por la Figura 21.

Country code	Regulatory class
2	1

Octets:

Figura 21: Elemento Regulatory domain

5.2.6 Capability network:

Este elemento de información que proporciona las capacidades de la red de cada una de las redes de una tecnología especificada en el “Info ID” del elemento ANQP.

Para este elemento utilizaremos el elemento de información especificado en 802.21 proporcionado por el MIIS “IE_NET_CAPS”. El formato del elemento Capacidades de la red se presenta en la Figura 22.

Network #1		
Length name	Name network	Capability network
1	variable	4

Octets:

Figura 22: Elemento Capacidades de la red

- “Length name” será la longitud del nombre de la red.
- “Name network” será el nombre de la red (definido por la respuesta MIHF “IE_NETWORK_ID”).
- “Capability network” proveerá las capacidades que soportara la red:
 - Bit 0: Security – Indicates that some level of security is supported when set.
 - Bit 1: QoS Class 0 – Indicates that QoS for class 0 is supported when set.
 - Bit 2: QoS Class 1 – Indicates that QoS for class 1 is supported when set.
 - Bit 3: QoS Class 2 – Indicates that QoS for class 2 is supported when set.
 - Bit 4: QoS Class 3 – Indicates that QoS for class 3 is supported when set.
 - Bit 5: QoS Class 4 – Indicates that QoS for class 4 is supported when set.
 - Bit 6: QoS Class 5 – Indicates that QoS for class 5 is supported when set.
 - Bit 7: Internet Access – Indicates that Internet access is supported when set.
 - Bit 8: Emergency Services – Indicates that some level of emergency services is supported when set.
 - Bit 9: MIH Capability – Indicates that MIH is supported when set.
 - Bit 10–31: (Reserved)

5.2.7 QoS:

Este elemento de información que proporciona la calidad de los servicios de cada una de las redes de una tecnología especificada en el “Info ID” del elemento ANQP.

Para este elemento utilizaremos el elemento de información especificado en 802.21 proporcionado por el MIIS “IE_NETWORK_QOS”. El formato del elemento Calidad de servicio se presenta en la Figura 23.

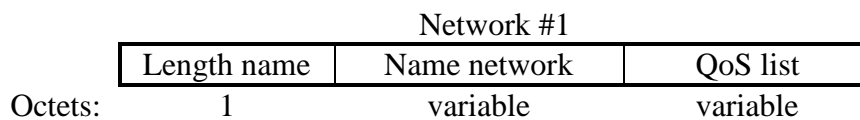


Figura 23: Elemento Calidad de servicio

- “Length name” será la longitud del nombre de la red.
- “Name network” será el nombre de la red (definido por la respuesta MIHF “IE_NETWORK_ID”).
- “QoS list” será una lista de de parámetros de CoS. El formato se presenta en la Figura 24.

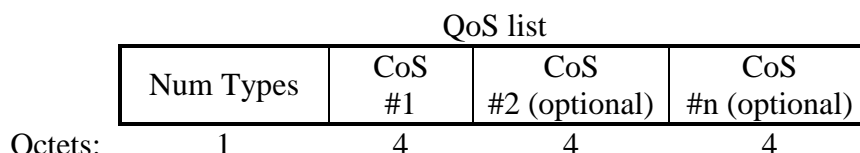


Figura 24: Elemento QOS list

- ❖ “Num Types” será el mayor numero de deferentes clases de servicios soportados y estará definido por la respuesta MIHF “IE_NETWORK_QOS->num_cos_types”.

- ❖ “Length” será la longitud del nombre de la red roaming.
- ❖ El formato de “CoS” esta definido en la Figura 25.

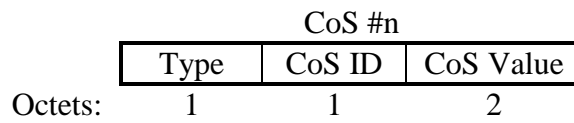


Figura 25: Elemento CoS

- ❖ “Type” será el tipo de la información referente a la CoS. Todos los tipos de información referentes a la CoS se definen en la Tabla 8.

Respuesta 802.21	Valor	Definicion
IE_NETWORK_QOS -> MIN_PK_TX_DELAY	1	A type to represent the minimum packet transfer delay in ms for the specific CoS specified by the COS_ID.
IE_NETWORK_QOS -> AVG_PK_TX_DELAY	2	A type to represent the average packet transfer delay in ms for the specific CoS specified by the COS_ID.
IE_NETWORK_QOS -> MAX_PK_TX_DELAY	3	A type to represent the maximum packet transfer delay in ms for the specific CoS specified by the COS_ID.
IE_NETWORK_QOS -> PK_DELAY_JITTER	4	A type to represent the packet transfer delay jitter in ms for the specific CoS specified by the COS_ID.
IE_NETWORK_QOS -> PK_LOSS_RATE	5	A type to represent the packet loss rate for the specific CoS specified by the COS_ID. The loss rate is equal to the integer part of the result of multiplying –100 times the log10 of the ratio between the number of packets lost and the total number of packets transmitted in the class population of interest.

Tabla 8: Tipos de CoS

- ❖ “CoS ID” será la clase de la cual nos informara de la capacidad y estará definido por la respuesta MIHF “IE_NETWORK_QOS->(Type)->cos_id”.
- ❖ “CoS Value” será el valor del tipo “type” de la clase “CoS ID” y estará definido por la respuesta MIHF “IE_NETWORK_QOS->(Type)->cos_value”.

5.2.8 IP Configuration:

Este elemento de información que provee información sobre las características y métodos de configuración de la dirección IP de la red.

Para este elemento utilizaremos los elementos de información especificados en 802.21 proporcionados por el MIIS “IE_NET_IP_CFG_METHODS” y “IE_NET_

MOB_MGMT_PROT”. El formato del elemento Configuración IP se presenta en la Figura 26.

Network #1			
Length name	Name network	IP Cfg Methods	Ip Mobility management
Octets: 1	variable	4	2

Figura 26: Elemento Configuración IP

- “Length name” será la longitud del nombre de la red.
- “Name network” será el nombre de la red (definido por la respuesta MIHF “IE_NETWORK_ID”).
- “IP Cfg Methods” será los métodos de configuración IP que tendrá la red. Los valores de cada método se definen en la Tabla 9.

Definicion	bit
Configuracion estatica IPv4	0
DHCPv4	1
FA-CoA	2
Co-located CoA	3
Reservado	4-10
Stateless address configuraiton	11
DHCPv6	12
Configuracion manual IPv6	13
Reservado	14-31

Tabla 9: Métodos de configuración

5.2.9 Frequency bands:

Este elemento de información proporciona una lista de frecuencias que soportan cada una de las redes de una tecnología especificada en el “Info ID” del elemento ANQP.

Para este elemento utilizaremos los elementos de información especificados en 802.21 proporcionados por el MIIS “IE_NET_FREQUENCY_BANDS”. El formato del elemento Bandas de frecuencia se presenta en la Figura 27.

Network #1					
Length name	Name network	Num frequency	Frequency #1	Frequency #2 (optional)	Frequency #n (optional)
Octets: 1	variable	1	4	4	4

Figura 27: Elemento Bandas de frecuencias

- “Length name” será la longitud del nombre de la red.
- “Name network” será el nombre de la red (definido por la respuesta MIHF “IE_NETWORK_ID”).
- “Num frequency” será el numero de frecuencias que tendrá la red.

- “Frequency #” será cada una de las frecuencias por las que se mantendrá conexión con la red, estas estarán definidas por “IE_NET_FREQUENCY_BANDS”.

5.2.10 PoA:

Este elemento de información proveerá de información relevante de todos los puntos de acceso que proveen servicio a cada una de las redes de una tecnología especificada en el “Info ID” del elemento ANQP.

Para este elemento utilizaremos el elemento de información especificado en 802.21 proporcionado por el MIIS “IE_CONTAINER_POA”. El formato del elemento PoA se presenta en la Figura 28.

Network #1					
Length name	Name network	Count PoA	PoA #1	PoA #2 (optional)	PoA #n (optional)
Octets: 1	variable	1	variable	variable	variable

Figura 28: Elemento PoA

- “Length name” será la longitud del nombre de la red.
- “Name network” será el nombre de la red (definido por la respuesta MIHF “IE_NETWORK_ID”).
- “Count PoA” será el numero de PoAs que pertenezcan a dicha red.
 “PoA #” será cada uno de los puntos de acceso definidos en la red. El formato se presenta en la Figura 29.

PoA #1					
Length	Link Addr	Location	Channel range	System info	Subnet info
Octets: 2	Variable	Variable	8	variable	33

Figura 29: Elemento PoA#N

- ❖ “Length” será la longitud de octetos del elemento POA
- ❖ “Link Addr” definirá el tipo de tecnología que utiliza el punto de acceso para definir la red. El formato de este elemento estará definido en la Figura 30 y el valor del campo Type estará definido en la Tabla 10.

Link Addr	
Type	Addr
Octets: 1	Variable

Figura 30: Elemento LinkAddr

Type	Value
MAC ADDR	0
3GPP 3G	1
3GPP 2G	2
3GPP ADDR	3

3GPP2 ADDR	4
OTHER L2 ADDR	5

Tabla 10: Tipo de link

- ❖ “Location” definirá la localización en la que se encuentra el punto de acceso. El formato del elemento esta definido en la Figura 31, Figura 32, Figura 33 y Figura 34, mientras que el valor de Type esta definido en la Tabla 11.

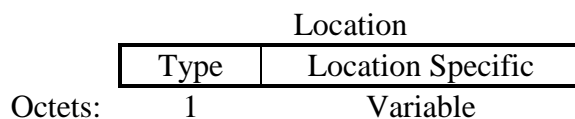


Figura 31: Elemento Location

Type	Value
BINARY CIVIC LOCATION	0
XML CIVIC LOCATION	1
BINARY GEO LOCATION	2
XML GEO LOCATION	3

Tabla 11: Tipo de Location

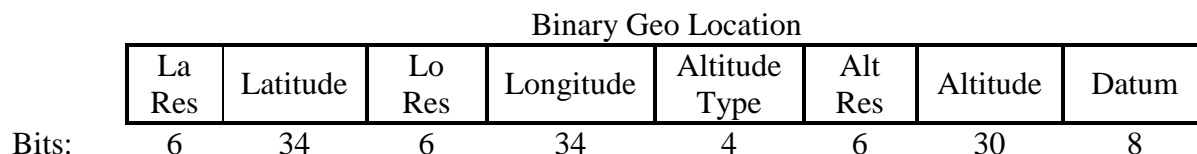


Figura 32: Elemento Binary Geo Location

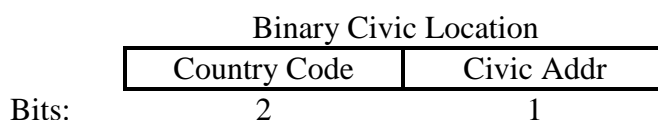


Figura 33: Elemento Binary Civic Location

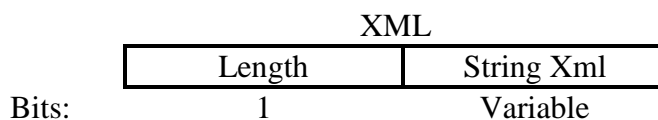


Figura 34: Elementos XML Location

- ❖ “Channel range” definirá la rango de frecuencias electromagnéticas por la que se interceptara el punto de acceso. Cada una de estas frecuencias será representada en Mhz. El formato del elemento esta definido en la Figura 35.

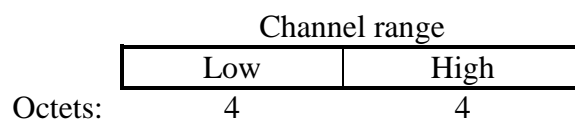


Figura 35: Elemento Channel range

- ❖ “System info” definirá información del punto de acceso (ID del sistema, banda de frecuencias que utiliza, clase de CDMA). El formato del elemento esta definido en la Figura 36.

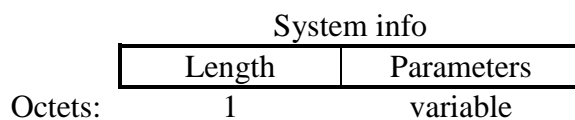


Figura 36: Elemento System info

- ❖ “Subnet info” indicara la subred que ofrecerá la red del punto de acceso. El formato del elemento esta definido en la Figura 37.

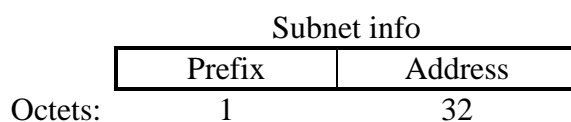


Figura 37: Elemento Subnet info

CAPITULO 6

PRUEBAS

6.1 Descripción del entorno de trabajo

Antes de empezar con las pruebas a realizar, describiremos el entorno de trabajo donde realizaremos dichas pruebas. Para ello utilizaremos dos equipos, uno portátil y otro de sobremesa, un teléfono móvil Samsung Galaxy SIII y 6 router Cisco WTR564L.

Para las pruebas de recopilación entre distintas tecnologías, conectaremos el equipo portátil, donde se encontrará el código 802.11u, a la red a través del teléfono móvil que se utilizara como punto de acceso. Será en este donde se determinara los diferentes tipos de tecnología a utilizar, ya sea wifi, 2G o 3G. Este teléfono conectara al equipo de sobremesa por su IP pública, donde correrá ODTONE para representar la red 802.21.

Para el descubrimiento de redes wifi, utilizaremos los routers como puntos de acceso a la red, donde con el equipo móvil mediremos el tiempo que necesitamos para descubrir todos.

Antes de empezar con las pruebas, también hay que resaltar que los datos estadísticos de dichas pruebas se mostraran en un “*plot box and whisker*” o también llamado diagrama de caja, donde las líneas superior e inferior mostraran el mínimo y el máximo valor hallado, donde la caja mostrara el 50% de los resultados hallados con el borde superior en el 3º cuartil y el inferior en el 1º cuartil, incluyendo una línea adicional mas en su interior que mostrara la mediana de los resultados hallados. Por ultimo destacar que los resultados atípicos hallados no serán mostrados en dichas graficas.

6.2 Recopilación de datos entre distintas tecnologías

La primera prueba que realizaremos será la de calcular cuanto tiempo necesita el nodo móvil en recopilar un tipo de información a través de la solución propuesta o a través del intercambio de paquetes 802.21 con tecnologías WiFi , tecnología GSM y tecnología UMTS.

Para ello realizaremos una misma pregunta utilizando un las distintas tecnologías. Para este caso utilizaremos por ejemplo el elemento ANQP “Name Network and name

network auxiliar” y para el caso de paquetes 802.21, utilizaremos la misma consulta SPARQL para mandar el paquete “MIH_Get_Information request”.

Utilizaremos un script en Linux basado en bash, donde ejecutaremos el programa correcto desde el comando “time” para calcular el tiempo que tarda el protocolo en recibir la respuesta. Este comando lo introduciremos en un while para ejecutarlo 50 veces y sacar resultados.

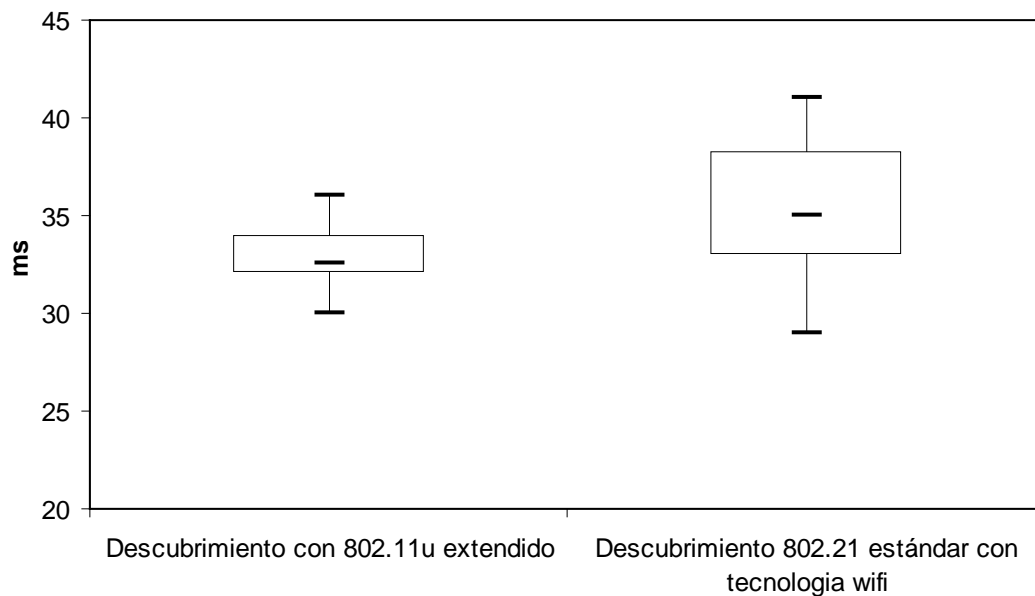


Figura 38: Relación entre el tiempo en ms. de la extensión ANQP y 802.21 con wifi

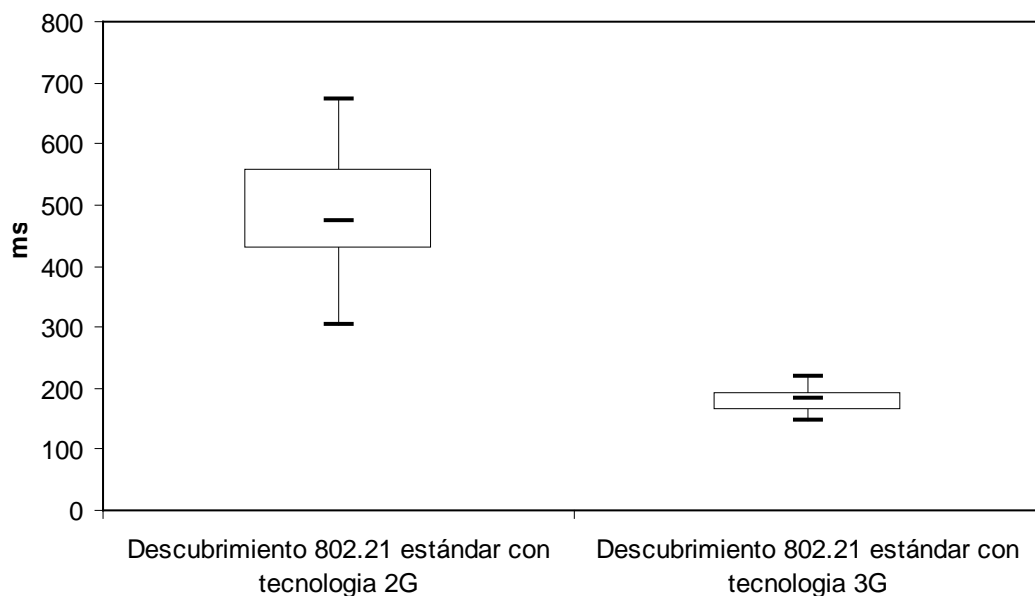


Figura 39: Relación entre el tiempo en ms. de las tecnologías 3GPP

Como observamos en las figuras 39 y 40, podemos observar que los resultados respecto al uso de cualquier tecnología para el descubrimiento de redes diferente a la tecnología wifi, sufre un retardo con respecto a la utilización de el protocolo propuesto,

ya que este utiliza tecnología wifi y su velocidad es considerablemente mayor. Además el uso de radiofrecuencias de tecnología wifi seria mucho menos costoso. Sin embargo, disponiendo de un nodo móvil capaz de utilizar 802.21, siempre utilizaríamos dicha tecnología puesto que es la más rápida y la menos costosa.

Respecto a la diferencia de tiempos con el uso de tecnología wifi, son diferencias irrelevantes puesto que no es un numero muy elevado de muestras, pero en ellas se puede observar perfectamente que el tiempo entre el intercambio de paquetes entre el nodo móvil y el punto de acceso es una diferencia minima de milisegundos, por lo que los tiempos de ambos protocolos serán prácticamente iguales, y el uso de 802.11 extendido no implicaría tener 802.21 integrado en el nodo móvil.

6.3 Descubrimiento de redes wifi

En esta prueba realizaremos un calculo entre la diferencia del tiempo que necesitamos para descubrir todas las redes IEEE 802.11 disponibles a través de la solución propuesta y a través del escaneo de todos los canales de radiofrecuencia wifi. Para ello, utilizaremos 6 router Cisco WTR564L, los cuales utilizaremos como puntos de acceso de los canales 1,3,5,7,9 y 11 (Ver Anexo III).

Para calcular el tiempo que tarda un nodo móvil en escanear todos los canales, utilizaremos un ordenador portátil en la cual crearemos una interfaz virtual la cual utilizaremos en modo monitor. Para ello, deshabilitaremos la interfaz “wlan”, crear la interfaz virtual y habilitar de nuevo la interfaz.

```
ifconfig <devname> down
```

```
iw dev <devname> interface add <name> type <type>
```

```
rkill unblock wifi
```

```
ifconfig <devname> up
```

```
ifconfig <name> up
```

Una vez creada, realizaremos un escaneo manual de todos los canales.

```
service network-manager stop
```

```
rkill unblock wifi
```

```
ifconfig wlan0 up
```

```
iwlist wlan0 scan
```

Observando el resultado en wireshark y el tiempo que tarda en realizar un escaneo completo es el de escanear los 11 canales, mientras que nosotros utilizaremos la media de canales por la probabilidad de que el canal sea el primero o el último.

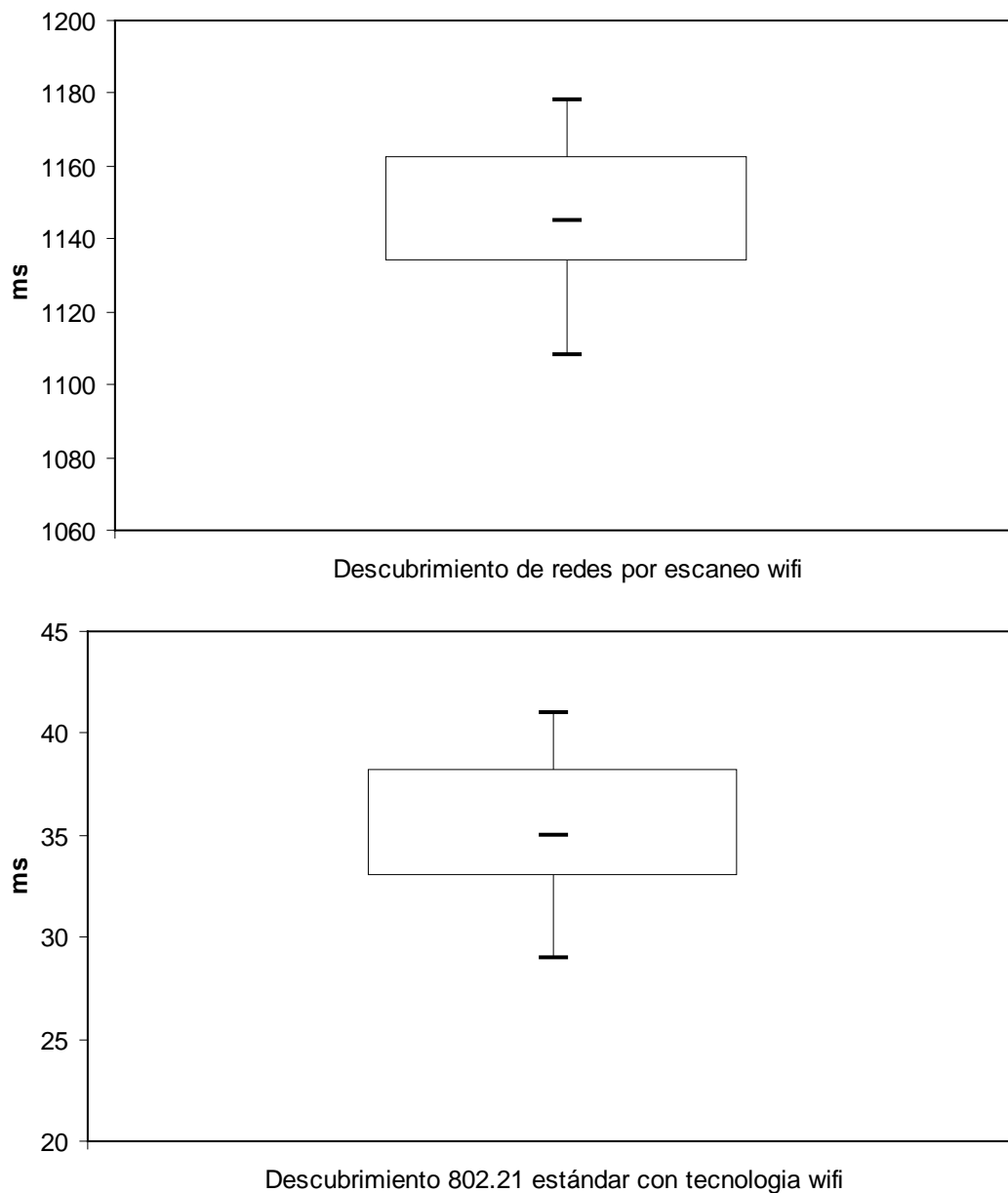


Figura 40: Relación entre el tiempo en ms. de el escaneo de redes wifi y la extensión ANQP

Observando la figura 40, observamos una amplia diferencia de tiempo a favor de la extensión ANQP en contra del uso de radio frecuencias, ya que además de tardar considerablemente menos incluiría información adicional a la que aportaría el uso de radiofrecuencias.

CAPITULO 7

CONCLUSIONES

El objetivo principal de este trabajo se presentó desde el principio como un análisis de la dificultad de acceder al Media Independent Information Service, proporcionado por IEEE 802.21, desde terminales que no implementaran dicha tecnología. Como punto de partida del trabajo, se ha supuesto el uso de una tecnología estándar como es IEEE 802.11u y su protocolo ANQP. Dicha tecnología forma parte de la especificación IEEE 802.11-2012 y debe de ser implementada en todos aquellos equipos que se vendan a lo largo del 2013 y en adelante³.

La primera conclusión del trabajo, es que la implementación de dicho servicio no es en absoluto trivial y aunque dicha comunicación se presupone compatible en los estándares IEEE 802.11u e IEEE 802.21⁴, los diversos Information Elements de cada tecnología no son directamente compatibles, como regla general.

Como una segunda parte de este trabajo, se ha realizado el diseño de los cambios necesarios en el protocolo ANQP para poder transportar los elementos de información definidos en IEEE 802.21 y se ha comprobado como el uso de información proporcionada por la red, acelera de manera substancial el descubrimiento de las redes de acceso.

Finalmente, merece la pena destacar, como la solución propuesta permite al terminal móvil beneficiarse de los servicios de descubrimiento extendidos proporcionados por IEEE 802.21, sin la necesidad de implementar dicho protocolo, lo cual debido a la elevada complejidad de dicho protocolo, permite reducir el coste del terminal.

³ Esta decisión se basa en las discusiones que se vienen manteniendo en diversos grupos de estandarización dentro del IEEE 802 y de la WiFi Alliance.

⁴ Por ejemplo, el estándar IEEE 802.21c, que se encuentra en su fase final de aprobación, incorpora un nuevo servicio de Proxy que supone la compatibilidad entre ambos protocolos.

ANEXO I

ODTONE

I.1 Descripción General

ODTONE (Open Dot Twenty ONE) es una implementación con código abierto de un Media Independent Handover Services (IEEE 802.21), implementada con una API C++.

Se utilizara esta implementación para desarrollar la mejora del protocolo GAS definida en este TFG. Este desarrollo será sobre un sistema GNU/Linux.

I.2 Dependencias de ODTONE

ODTONE requiere la utilización de la librería Boost 1.47 o superior.

Boost es un conjunto de bibliotecas de software libre preparadas para extender las capacidades del lenguaje de programación C++ con licencia de tipo BSD, que permite que sea utilizada en cualquier tipo de proyecto.

Descargaremos la librería de su página oficial:

<http://www.boost.org/>

Una vez descargada, procederemos a instalarla en nuestro sistema. Por ejemplo utilizaremos una carpeta en el directorio home de nuestro usuario llamada “proyecto” donde descomprimiremos las librerías. De forma siguiente abriremos la carpeta tools/build/v2 de dicha librería, ejecutaremos el script “bootstrap.sh” y procederemos a realizar la opción de instalar:

cd ~/proyecto/boost_v1.47/tools/build/v2

./bootstrap.sh

sudo ./b2 --install

De esta forma tendremos instalada las librerías de boost necesarias para compilar ODTONE. Para dicha compilación utilizaremos el siguiente comando:

./b2 ruta_de_compilacion

I.3 Compilación e instalación de ODTONE en GNU/Linux

Descargaremos ODTONE de su página de proyecto.

<http://helios.av.it.pt/projects/odtone/files>

Nos descargaremos la última versión que se encuentre disponible, en nuestro caso “odtone-src-v0.4.tar.bz2” y la colocaremos siguiendo la misma estructura que con la librería boost, por lo que la colocaremos en la carpeta “odtone” dentro de la carpeta “proyecto”.

Una vez colocada procederemos a compilar ODTONE. Para ello utilizaremos el método anteriormente explicado:

cd ~/proyecto/boost_v1.47/tools/build/v2

*./b2 ~/proyecto/odtone/app/**

*./b2 ~/proyecto/odtone/src/**

En el caso de tener que utilizar algún tipo de librería externa a ODTONE, en el momento de la compilación introduciremos la siguiente opción:

-- linkflags="librería_externa".

Una vez realizado esto se creará automáticamente la carpeta “bin.v2” donde se colocaran los binarios de ejecución.

I.4 Estructura de ODTONE

Sin contar librerías, ODTONE se estructura en 3 carpetas: “src”, “app” y “bin.v2”. Como ya hemos comentado anteriormente en “bin.v2” se encontraran todos los ejecutables que se crearan al instalar dicha implementación.

En este proyecto utilizaremos un cliente MIH, el MIIS y un MIFH por lo que solo procederemos a instalar cada uno de estos, lo que implicará que solo instalaremos “src/mihf”, “app/miis” y “app/client”. De esta forma tendremos creado una estructura básica 802.21 donde podremos realizar preguntas 802.21 desde el cliente al MIHF.

ANEXO II

SPARQL

II.1 Generación de base de datos para ODTONE

Para la reproducción del protocolo establecido necesitaremos utilizar datos introducidos en el MIIS.

ODTONE proporciona una base de datos para el uso del protocolo muy reducido, por lo que necesitaremos generar nuestra propia base de datos para realizar las pruebas. Para ello tendremos que utilizar dos archivos:

- base_schema.xml
- data.ttl

El esquema de esta base de datos estará definido por la estructura de la especificación IEEE 802.21, archivo que podremos encontrar en la implementación de ODTONE.

Los datos de dicha base serán introducidos a través de el archivo data.ttl, el cual tendremos que realizar. Para la realización de nuestras pruebas utilizaremos el siguiente ttl (solo especificaremos una única red):

prefix : <http://www.mih.org/2006/09/rdf-basic-schema#> .

```
<network1>
  :ie_network_id "network1";
  :ie_network_aux_id "aux_id_1";
  :ie_cost [
    :cost_currency "USD";
    :service-info "1";
    :cost_unit "2";
    :cost_value "5" ];
  :ie_network_type [
    :link_type "23" ];
  :ie_operator_id [
    :op_name "red-mobile";
    :op_namespace "0" ];
  :ie_container_poa [
```

```

:ie_poa_link_addr [
  :link_addr_3gpp_3g [ :link_addr_3gpp_3g_cell_id_plmn_id "bbb" ];
  :address-type "6" ];
:poa-capabilities "004a";
:ie_poa_channel_range [
  :high_ch_range "470";
  :low_ch_range "450" ];
:poa-data-rate "50";
:ie_poa_location [
  :BIN_GEO_LOC [
    :altitude "0f00";
    :alt_res "30";
    :at "1";
    :datum "1";
    :latitude "04dcc1fc8";
    :la_res "21";
    :longitude "f65ecf031";
    :lo_res "20" ];
  :method "0" ];
:poa-mac-type "CSMA-CA";
:ie_poa_subnet_info [
  :ip_subnet_info "16";
  :subnet_address [
    :add_value "c0230000";
    :add_family "1" ]
  ] ];
:qos "class1/class2/class3";
:ie_roaming_partners [
  :op_name "red-partner1";
  :op_namespace "0" ],
  [
    :op_name "red-partner2";
    :op_namespace "1" ]; .

```

Para la generación de la base de datos en si, deberemos ejecutar el siguiente comando:

```
rdfproc -n nombre -s sqlite parse data.ttl turtle base-schema.xml
```

De esta forma se generara la base de datos que utilizaremos al ejecutar el MIIS.

II.2 Consultas SPARQL para cada elemento ANQP

Una vez que hemos definido la base de datos que tendrá el MIIS, definiremos cual serán las consultas SPARQL para cada uno de los paquetes definidos en la extensión de los elementos ANQP.

- Name network and name network auxiliar:


```

PREFIX mihbasic: <http://www.mih.org/2006/09/rdf-basic-schema#>
SELECT ?network_id ?network_aux
WHERE
{
  ?network mihbasic:ie_network_id ?network_id .
  ?network mihbasic:ie_network_type ?network_type .
  ?network_type mihbasic:link_type ?link_type .
  FILTER regex(?link_type, tecnologia) .
  ?network mihbasic:ie_network_aux_id ?network_aux .
}

```

- Roaming patners:

```

PREFIX mihbasic: <http://www.mih.org/2006/09/rdf-basic-schema#>
SELECT ?network_id ?opname ?opnamespace
WHERE
{
  ?network mihbasic:ie_network_id ?network_id .
  ?network mihbasic:ie_network_type ?network_type .
  ?network_type mihbasic:link_type ?link_type .
  FILTER regex(?link_type, tecnologia) .
  ?network mihbasic:ie_roaming_partners ?partners .
  ?patners mihbasic:op_name ?opname .
  ?patners mihbasic:op_namespace ?opnamespace .
}

```

- Cost network:

```

PREFIX mihbasic: <http://www.mih.org/2006/09/rdf-basic-schema#>
SELECT ?network_id ?cost_unit ?cost_value ?cost_curr
WHERE
{
  ?network mihbasic:ie_network_id ?network_id .
  ?network mihbasic:ie_network_type ?network_type .
  ?network_type mihbasic:link_type ?link_type .
  FILTER regex(?link_type, tecnologia) .
  ?network mihbasic:ie_cost ?cost .
  ?cost mihbasic:cost_unit ?cost_unit .
  ?cost mihbasic:cost_value ?cost_value .
  ?cost mihbasic:cost_curr ?cost_curr
}

```

- Country code:

```

PREFIX mihbasic: <http://www.mih.org/2006/09/rdf-basic-schema#>
SELECT ?network_id ?country_code
WHERE
{

```

```

?network mihbasic:ie_network_id ?network_id .
?network mihbasic:ie_network_type ?network_type .
?network_type mihbasic:link_type ?link_type .
FILTER regex(?link_type, tecnologia) .
?network mihbasic:ie_country_code ?country_code .
}

```

- Regulatory domain:

```

PREFIX mihbasic: <http://www.mih.org/2006/09/rdf-basic-schema#>
SELECT ?network_id ?regulatory_class ?country_code
WHERE
{
  ?network mihbasic:ie_network_type ?network_type .
  ?network_type mihbasic:link_type ?link_type .
  FILTER regex(?link_type, tecnologia) .
  ?network mihbasic:ie_net_regulat_domain ?regulat_domain .
  ?regulat_domain mihbasic:country_code ?rcountry_code .
  ?regulat_domain mihbasic:regulatory_class ?regulatory_class .
}

```

- Capability network:

```

PREFIX mihbasic: <http://www.mih.org/2006/09/rdf-basic-schema#>
SELECT ?network_id ?net_caps
WHERE
{
  ?network mihbasic:ie_network_type ?network_type .
  ?network_type mihbasic:link_type ?link_type .
  FILTER regex(?link_type, tecnologia) .
  ?network mihbasic:ie_net_caps ?net_caps .
}

```

- QoS:

```

PREFIX mihbasic: <http://www.mih.org/2006/09/rdf-basic-schema#>
SELECT ?network_id ?cos_id ?cos_value
WHERE
{
  ?network mihbasic:ie_network_type ?network_type .
  ?network_type mihbasic:link_type ?link_type .
  FILTER regex(?link_type, tecnologia) .
  ?network mihbasic:ie_network_qos ?network_qos .
  ?network_qos mihbasic:cos_id ?cos_id .
  ?network_qos mihbasic:cos_value ?cos_value .
}

```

- IP Configuration:

```
PREFIX mihbasic: <http://www.mih.org/2006/09/rdf-basic-schema#>
SELECT ?network_id ?mob_mgmt_prot ?cfg_methods
WHERE
{
  ?network mihbasic:ie_network_type ?network_type .
  ?network_type mihbasic:link_type ?link_type .
  FILTER regex(?link_type, tecnologia) .
  ?network mihbasic: ie_net_ip_cfg_methods ?cfg_methods.
  ?network mihbasic: ie_net_mob_mgmt_prot ?mob_mgmt_prot.
}
```

- Frequency bands:

```
PREFIX mihbasic: <http://www.mih.org/2006/09/rdf-basic-schema#>
SELECT ?network_id ? frequency_bands
WHERE
{
  ?network mihbasic:ie_network_type ?network_type .
  ?network_type mihbasic:link_type ?link_type .
  FILTER regex(?link_type, tecnologia) .
  ?network mihbasic: ie_net_frequency_bands ? frequency_bands.
}
```

ANEXO III

RESTAURACION DE UN LINKSYS WRT546L

III.1. Linksys WRT546L

Para la realización de las pruebas de este proyecto, se necesitara utilizar como punto de acceso varios router Linksys WRT546L. Estos router son de uso de la universidad por lo que al recibirlos no sabemos ninguna dirección de sus interfaces ni la contraseña que tiene al entrar en el.

III.2. Instalación de un nuevo firmware

Para restaurar el router, instalaremos un nuevo firmware entrando como “fail safe mode”.

Este firmware lo obtendremos de la siguiente forma:

```
cd tmp
```

```
http://downloads.openwrt.org/whiterussian/newest/default/openwrt-brcm-2.4-squashfs.trx
```

Para entrar en el modo “failsafe” pulsaremos el botón de reinicio estando el router desenchufado de la corriente, sin soltarlo, enchufaremos el router a la corriente hasta que la luz marcada como “DMZ”. En ese momento relajaremos el botón de reset. Si lo hemos hecho bien, las luces de “POWER” y “DMZ” empezaran a parpadear.

Una vez puesto el router en modo “failsafe”, conectaremos nuestro PC a cualquiera de sus interfaces, donde podremos entrar a través de el por la dirección 192.168.1.1, sin olvidarnos por supuesto que para realizar un telnet a la dirección 192.168.1.1 nuestra interfaz del PC deberá tener una dirección IP que este en red local con dicha dirección, por ejemplo la 192.168.1.2.

Ya dentro del router introduciremos las siguientes líneas:

```
cd tmp
```

```
scp root@192.168.1.2:/tmp/openwrt-brcm-2.4-squashfs.trx ./
```

```
mtd -r write openwrt-brcm-2.4-squashfs.trx linux
```

Una vez realizado esto, automáticamente el router se reiniciara de tal forma que podremos introducirnos por sus interfaces como recibido de fábrica.

BIBLIOGRAFIA

- Estándar 802.11
- Estándar 802.21
- <http://standards.ieee.org/>
- <https://openwrt.org/>
- <http://www.ieee802.org/11/>
- http://www.it.uc3m.es/aoliva/pdf/wcm_80221.pdf
- <http://skos.um.es/TR/rdf-sparql-query/>
- <http://hng.av.it.pt/projects/odtone>
- <http://helios.av.it.pt/projects/odtone/>

AGRADECIMIENTOS

Antes de terminar, me gustaría dar las gracias a cada una de las personas que a lo largo de mi vida me han hecho llegar a donde estoy ahora, paso a paso he llegado gracias a todos ellos.

Los primeros mis padres, a mi abuela y mi hermano, que gracias a ellos soy la persona que soy, que me han cuidado como nadie lo hubiera hecho, me han dado todo, y no sería la mitad de persona si no fuera por todo lo que han hecho. Nunca tendría palabras suficientes para agradecerérselo, gracias.

Gracias a Adri, Aitor, Alberto, Munitis, Are, Antelo, Jose, Tron, Javi, Richi, Tito, Zurita y sobre todo a Pablo, por que sin ellos no habría acabado la carrera todavía, por que aparte de apoyarme siempre me alegraban cada día en la universidad.

Gracias a mis dos tutores, Antonio y Carlos, y sobre todo a Antonio, que me ha tenido que aguantar un año para este trabajo y me ha guiado para que todo salga perfecto, su dedicación ha sido crucial y este trabajo es más suyo que mío.

Sin olvidarme de todos vosotros, todos mis amigos, que aunque les odie, no tengo palabras para describir todo lo que han hecho por mí y lo mucho que me importan.

Y sobretodo, gracias a ti, por aparecer en mi vida.